Data protection anno 2014: how to restore trust? – An introduction

Hielke Hijmans and Herke Kranenborg

1. Introduction

In the five decades during which Peter Hustinx has worked in the field of privacy and data protection many things have changed, as was eloquently stipulated in the preface by vice-president Reding.

Peter Hustinx started his career at a moment a debate took place at national as well as European level on whether the right to privacy as the 'right to be left alone' was still capable of facing the challenges posed by the development of information technology. Automated data processing was done in a way one could understand what data were involved, who was processing the data and where the processing took place. At the time, when Peter Hustinx took the train to Strasbourg to negotiate the Council of Europe Convention 108 on data protection, without being disturbed by a ringing mobile phone or incoming mail on his tablet, would he have realised the world would develop as it has done?

Privacy and data protection were rather unknown concepts, at least to the public at large. Today, we live in an era in which issues relating to privacy and data protection are daily news items.

This might be seen as a positive tendency because it confirms that finally the values behind privacy and data protection are taken seriously in wide circles of our societies. However, issues relating to privacy and data protection are not necessarily newsworthy because these rights have been so well protected. It is the scandals that make the news. This creates a feeling of uncomfortableness: there is a growing perception that the processing of personal data is out of control and that it is extremely difficult to get this control back.

The latest example of such a scandal took place in 2013, the last year of Peter Hustinx' mandate, concerning the US National Security Agency (NSA). Leaked documents revealed mass surveillance activities performed by the NSA on citizens in countries all over the world. It led to world wide criticism and heated public debates. From a more neutral perspective, the NSA-case can be seen as an illustration of the huge global societal challenges we are facing today. It reveals several phenomena that charactarise the society we currently live in. In the next paragraph we will briefly discuss five of these phenomena.

2. Five phenomena demonstrated by the NSA-case

Data are everywhere

The NSA-case shows in the first place that data are everywhere. This has fundamentally changed our society. Due to phenomena like cloud computing, data are no longer linked to one physical location, but are present at multiple places around the globe. We continuously produce data, be it in social networks, on search engines or through mobile apps, but we are not aware of all what happens with these data. However, all these data – one nowadays speaks about 'big data' – have value, for private companies as well as for governments. Data are quite often referred to as the new gold, or as Jones Harbour puts it in her contribution the new oil of Internet, exactly because technology allows surveillance (be it for behavioural advertising or for public security, or any other purpose). Since data are everywhere, the economic and public security incentive is to use them extensively and for multiple purposes.

Boundaries between private and public sector data processing are blurring

In the second place, the NSA-case illustrates that the traditional bounderies between private and public sector data processing are blurring. Many legal instruments make strict distinctions between private and public actors. For example, the law enforcement sector is excluded from the proposed General Data Protection Regulation (GDPR)[1] and, in relation to the fundamental rights protection in the EU, as well as in the US, it is argued that this protection does not (fully) work in horizontal relations between citizens and companies.[2] However, in practice, governments make more and more use of data that are collected in the private sector. Initiatives to allow and regulate such practices have created the most prominent public debates on data protection in the past years. Next to the NSA-case, mention can be made of access to financial transaction data, to airline passenger data (PNR) and to mobile telephone and internet data. It should be underlined that this phenomena is equally emerging on both sides of the Atlantic Ocean.

There is a huge gap between law on paper and the application of the law in practice

Amongst these matters the NSA-case takes a special position as it reveals another, third issue, namely that there is a big gap between the law on paper and the application of the law in practice, at least from a European perspective. We are faced with the limits of governments' competences.

In the first place, more in general, governments are less and less in a position to govern through traditional legislative instruments, because of the complexity of the issues, the speed of the introduction of ever more new technologies and the necessarily slower pace of the legislative process, which requires reflection and consultation of interested parties, before laws are adopted. The laws itself are not always capable to capture developments in society,

[1] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.01.2012, COM(2012) 11 final.

[2] See on this contributions of Verhey and of Kokott/Sobotta, on the Charter of the fundamental rights of the Union, and of Weitzner on the US Constitution.

and thus to be applied effectively. This is one of the reasons why so much effort is put in the concept of accountability, as described in the contribution of Thomas, making organisations themselves responsible.

Moreover, since data are everywhere, governments are not fully capable to enforce the laws and their underlying values. National governments as well as the EU struggle in finding ways how best to protect their citizens, necessarily also outside of their geographical territory. This is not only a problem in the EU, but equally in the US. The main players on the internet operate globally: data controllers are subject to different jurisdictions, sometimes with conflicting obligations. For the EU there is an additional challenge, based on the fact that it lacks full competence in areas where national security is involved. Article 4 TEU considers this as an area of essential state function, which belongs to the domain of the Member States. Also the annulment of the first PNR-agreement between the EU and the US, as Docksey highlights in his contribution, was the consequence of lacking competence with a result that the EU was no longer capable to deliver full protection.

Global convergence about basic values, but divergence in delivery

In the fourth place, the NSA-case also shows that in many parts of the world there actually is convergence about the basic values that need protection. This is undoubtedly the case when we compare the EU and the US which use similar concepts of privacy, as is underlined in the contributions of Brill and of Swire. The Obama-paper[3] and the recently adopted OECD-guidelines demonstrate this convergence.[4]

However, there may be divergence in how to deliver these values in practice, and how to balance competing interests. This is of particular interest in the relation between the EU and the US, where we may have different stakes in the balancing between privacy and security. NSA brings to light in its clearest form the outweighing between privacy and data protection on the one hand, and national security on the other hand. Most of us accept that security services need to use modern technologies to do their job and to protect our societies against possible attacks, whereas we also – on both sides of the Atlantic - contest the need to monitor on a massive scale.[5]

Trust is diminishing

In the fifth place, the NSA-case illustrates diminishing trust. Diminishing trust of citizens in the companies they deal with, diminishing trust in their governments, diminishing trust in

[3] "Consumer Data Privacy in a Networked World", available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.
[4] Available at: <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>.
[5] See contribution P.J. HUSTINX to LIBE Committee Inquiry on electronic mass surveillance of EU citizens, available at: <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf>.

supranational entities such as the EU, diminishing trust in the law, diminishing trust between countries. A lack of trust is detrimental for a society. It is clear that action should be taken to restore such trust. In her contribution, Prins argues that there is no master plan leading to this massive data processing and that governments have no overview of all the information they are collecting and using for different purposes. Big brother may thus be an illusion. However, the data is out there and current technology enables public authorities and private internet companies that have the capacity to collect and analyse massive amounts of data to become instant big brothers which are not necessarily under full control of parliaments and/or the judiciary.

These two dimensions, which can be seen as two sides of the same medal, contribute to the diminishing trust. Governments lack overview and cannot offer sufficient protection to their citizens. At the same time other players – that are not necessarily under full control of parliaments and/or the judiciary – have the overview and may take control over massive amounts of individual's personal data.

3. This book

This book comes at a moment, we are still in the middle of the global debate on the NSA-case. The five phenomena just sketched out charactarise the current society, but should not be taken for granted. They pose challenges which should be faced. The title of this book refers to perhaps the most emminent challenge, namely to restore trust. In our view governments have to show that the matter is not growing out of hand and should regain control by ensuring the issue is fully governed by the rule of law.

It has become clear that the processing and the protection of personal data is a subject of general importance and concern for everyone: for citizens and companies, for governments, for judges, for supervisors and for other stakeholders. This book brings together authors representing many of these stakeholders within Europe and in the US. Many of the contributions in this book refer to one or more of the phenomena just discussed, either by describing these phenomena, by describing the action that is currently taken or by giving directions on how to face the challenges.in the time ahead of us.

We have chosen to divide the book in six parts.

Fist part: Introduction

Next to the present contribution, the first part contains a contribution from Prins on iGovernment in which she illustrates the complexity of the subject. What we basically learn from the example of iGovernment is that we live in an era of big data, where systems are created, data are exchanged, new technologies are exploited, and this all without any central overview, without a "bigger picture". The risk is not so much that one big organisation ("big brother") determines what happens in the information society, but that many develpments

take place, simultanuously and in an uncoordinated way, with as a result that control becomes almost fictitious. This example sets the scene for the perspective of this book. How to restore trust and regain control?

Second part: Observations from nearby

The second part of this book is more an illustration of the change in society, and of the area of data protection, during the decades Peter Hustinx was active in this area, in particular as Data Protection Commissioner. The contributions are made by three persons who witnessed those activities from very nearby, namely as his deputies. Van de Pol was his deputy from 1994 till 2003 at the Dutch Data Protection Authority, whereas Bayo Delgado (2004-2009) and Buttarelli (2009-2014) served as assistant EDPS. Van de Pol explains the uphill battle a data protection authority has to fight, in particular to ensure that the values of privacy and data protection are not easily outweighed against competing interests. He focuses on the law enforcement sector, where privacy was regularly positioned as complicating police work and security. His conclusion that this will always be an unequal debate may be true, but the issue for the future will be whether the NSA case does not – to certain extent at least – changes the public perception.

Another dimension of this uphill battle follows the contribution of Bayo Delgado. As a supervisor – and in his case a newly appointed supervisor at EU level, starting from scratch - the question arose whether a battle should be fought and whether promoting data protection would not be best achieved by being available for consultation, or, if we put it in a provocative manner by being part of the system instead of fighting the system. It is a much wider issue: choosing for pragmatism and integrating data protection in organisations, in an attempt to regain control, may be the most effective manner to achieve results.
An example of integrating data protection in the system is the subject addressed by Buttarelli, data protection in the judicial procedure. [PM***]

Third part: Constitutional values and the role of the judiciary

The third part focuses on the societal values of privacy and data protection, as they are protected in our constitutional systems, in constitutional and other laws, and by Courts. The examples Verhey gives us on the debate on the Dutch Constitution illustrate that underlying values may be static – already the Constitution of 1815 contained a provision, which could be seen as aiming at protecting privacy – but that constitutional provisions may need revision as time evolves, in order to remain effective. He also addresses another recurring discussion around the constitutional protection of data protection. Is the right to data protection a directly applicable fundamental right of the citizen or is it meant as instruction to the legislator to ensure protection? A similar discussion is taking place in the EU context, around Article 8 of the Charter of the Fundamental Rights of the Union. Finally, there is the issue of the horizontal effect of constitutional provisions. Do they only protect against governments or also in “horizontal” relations between private parties.

Kokott and Sobotta also discuss this horizontal effect (or "Drittwirkung") and come to the conclusion that Article 8 of the Charter may not apply in horizontal relations, because the Charter itself is addressed to EU bodies, and to the Member States when they are implementing EU law. This is an interesting view, also in light of the Court's judgement in *Akerberg Fransson* where it states that "situations cannot exist which are covered in that way by European Union law without those fundamental rights being applicable."[6] The main element of this contribution however is the distinction between privacy and data protection, and the importance this distinction can have in practice. This distinction is something Peter Hustinx also defends, e.g. in relation to the *Bavarian Lager* ruling of the Court of Justice of the EU, in which the EDPS was involved in several instances.[7] The objectives of data protection do not always coincide with the values behind privacy.

Docksey discusses the role of the Court of Justice of the EU, focussing on a few landmark cases that are decisive for determining the scope of the rights to privacy and data protection, and for the competence of the EU to effectively protect. He shows that the Court of Justice in his earlier cases interpreted the scope of the right to data protection in a wide manner, and decided that the Union should protect, also in cases where the EU competence is not obvious[8]. However, it opted for a formalistic, non protective approach in the PNR case, whilst protection of EU citizens was even more needed since the case concerns the transfer of personal data to public authorities (in the US) in the framework of law enforcement, and thus processing by the public sector in a potentially sensitive area.

Rotenberg [PM***]

Fourth part: Role of the legislator and independent control

Part 4 of the book focuses on the role of the legislator, on various issues relating to effective law making, relating to this complex environment, and to the role of the supervisory authorities.

Albrecht gives an overview of the proposed general data protection regulation, and reasons why this initiative deserves support. He explains key issues such as the importance of uniform data protection law and consistency in enforcement of the law, e.g. through the proposed consistency mechanism. He also emphasises that for the European Parliament national specificities should be exceptional. Moreover, he mentions that the new regulation should not lead to a lower level of protection compared to Directive 95/46/EC. This is a risk

[6] CJEU, Case C-617/10, *Åklagaren v. Hans Åkerberg Fransson, n.y.r.*
[7] CJEU, Case 28/08 P, *European Commission v. Bavarian Lager*, [2010] ECR I-6055.
[8] Directive 95/46/EC was based on an internal market legal basis, which was before the Lisbon Treaty the main legal basis to regulate data protection on EU level. The CJEU rulings in the cases *Lindqvist* and *Rundfunk*, as explained by Docksey, concern facts that do not affect the functioning of the internal market.

that is quite consistently mentioned by German participants in the debate, this country having the most elaborate system of data protection in the EU, and possibly in the world.

This specific German situation, where sub-national laws exist in 16 Länder, is further explained in the contribution by Dix. According to Dix this federalism – which also includes sub-national data protection authorities –does not stand in the way of harmonisation cross Europe. However, he also pleads for flexibility within the EU, in any event for the public sector. This contribution would lead to further thinking whether national an sub-national flexibility would be helpful for the data subjects in those areas, or whether it would jeopardise the effectiveness of the protection as such when citizens are not equally protected in all Member States – and parts of Member States – of the EU.

The next issue relates to the substance of the data protection laws. We earlier stated that the laws itself are not always capable to capture developments in society, and thus to be applied effectively. A solution to deal with this problem is to find an alternative to command and control laws, such as putting the emphasis on the principle of accountability,which is described by Thomas. Accountability is an approach which has always been strongly supported by Peter Hustinx – as a modern approach to legislation and which aims at lying the responsibility where it belongs, namely the data controller, and avoiding that data protection authorities wil be considered as primary reponsible for data processing, a task they reasonably can not fulfil.

Accountability means that organisations have to organise data protection and demonstrate how they do this, but they are free to choose the means. Thomas indicates how accountability could work. What is interesting in this concept is to find solutions ensuring that the efforts organisations have to make in ensuring accountability relate directly to the risk a processing operation poses to (the privacy of) the individual.

Effective protection also requires that it is well ensured that there is clarity about the interpretation of the necessarily general provisions of data protection law. Of course, within the EU uniform interpretation is at the end of the day a task of the Court of Justice, but guidance by data protection authorities – an in particular the Article 29 Working Party – has always been a strong incentive for effective protection. The contributions by Kohnstamm and by Moerel have this informal harmonisation by the Working Party – that will remain equally important under the new Regulation - as their subject.

Kohnstamm highlights the contributions by Peter Hustinx to this quite often labour intensive development of practical guidance on key data protection provisions. He mentions guidance on issues like the conceopt of personal data, consent and purpose limitation. This guidance is very influential for data protection practitioners, but can also serve in the discussions on the new data protection framework. For example, on the basis of the work on key provisions the attacks on purpose limitation in the debate on the new framework could be efficiently countered. Purpose limitation is one of the most fundamental elements of protection for the

data subject, whereas on the other hands limitations on purpose and thus limiations on further use of data are counter-intuitive for data controllers and processors.

Finally, Moerel discusses one specific item, namely the applicability of Directive 95/46, as well as the General Data Protection Regulation (GDPR) in situations where the controller and/or the processor is not established in the EU. She tries to solve a long standing debate between her and Peter Hustinx relating to Article 4 of Directive 95/46, which is in particular relevant in relation to different variations of outsourcing. She criticises how the opinion of the Article 29 Working Party on Swift[9] in her view did not do justice to the concepts of Article 4, and thus jeopardises the effectiveness of EU law.

Fifth Part: The transatlantic perspective

[PM In 't Veld]

Part 5 deals with the relations between the EU and the US, but from a wider perspective than the NSA case. Several contributions give the perspective of the US, and describe the long standing traditions on privacy, different but not necessarily worse than what Europe does.

How to better start American privacy than with Brandeis, who for the first time argued that persons have "a right to be left alone"? Brill recalls that his first concerns on privacy already already relate with upcoming techologies, such as in 1890 the snapshot photography. She explains how the Federal Trade Commission – also a child of Brandeis – concentrates o privacy, and how its enforcement actions resulted in severe orders against a few internet giants. The next and important step she addresses is the enforcement cooperation. Effective cooperation between enforcement agencies, cross borders and cross continents, is an important mechanism in restoring trust and regaining control. The OECD supported Global Privacy Enforcement Network (GPEN) initative is something that needs full support.

She also describes the protection in the US, and the Consumer Privacy Bill of Rights, following the 2012 Obama paper,[10] and comes up with a widespread cliché, namely that we should have EU laws and US enforcement.

Clichés about the contrast between the EU and US approaches are the topic of the contribution of Swire, who also praises the knowledge and understanding of Peter Hustinx of US law, and the need for a transatlantic debate. He describes the cliché that in the US protection would not be based on fundamental rights, that equally legislation is replaced by multistakeholder approaches, and finally that Europe would be less concerned about

[9] Opinion 10/2006 of the Article 29 Working Party of on the processing of personal data by the Security for Worldwide Interbank Financial Telecommunication (SWIFT),WP 128, 22.11.2006, available at: < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf >.

[10] The paper "Consumer Data Privacy in a Networked World" is available at: <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

invasions by government than by big private companies. The last cliché is debatable, but – indeed – we see in the EU a constant push back when it comes to regulating data protection in the sector of police and justice. The resistance in Council against the proposed directive for data protection in that sector is a good example. For EU Member States it is not always obvious that data protection in the police sector should be subject to stringent EU rules, or even more fundamentally, be subject of EU intervention as such.

Weitzner continues this discussion, brings forward the Obama-paper as well, and notes that the biggest progress in the US is in the area of consumer privacy, an area where the US Constitution does not protect. Progress is made e.g. through strong enforcement by the Federal Trade Commission. He also makes the link to the NSA case, which we took as the example that shows the challenges we are faced with today. This case makes even more clear why a close cooperation between those working on privacy and data protection on both sides of the Atlantic is needed, based on a good understanding of each others' systems.

Kuner's analysis on the protection of foreign nationals in EU and US data protection law is in that respect very helpful. He starts from the basic assumption that in the EU the protection stems from the European Convention on Human Rights and Fundamental Freedoms (ECHR) and thus protection is given irrespective of nationality. In the US, it is the approach of the US Supreme Court that differentiates in a numer of cases between US nationals and aliens. However, his contributions show that in practice both systems have indeficiencies as concerns extending protection to aliens, which has got a news dimension on Internet.

The contribution of Jones Harbour focuses on a relatively new issue, which triggers the discussion more and more on both sides of the Atlantic. This is the relationship between data protection and competition. She notes that personal data are becoming an increasingly important asset on the internet, whereas internet companies increasingly compete in multiple markets, and mentions the shift to mobile computing as giving this all new dimensions. Finally, where the internet market is dominated by a few players that have market dominance, those do not feel the incentive to respect high privacy standards in order to get competitive advantage.

Sixth part: The contributions of the European Data Protection Supervisor

Part 6 describes how the EDPS has contributed in the ten years of Peter Hustinx, and how respect of data protection is ensured within the institutions.

De Hert and Papakonstantinou characterise the EDPS as a unique stakeholder in the European data protection landscape, and address his role as an EU advisor 'on all matters concerning the processing of personal data'. They start their contribution with the reversal of the general data protection environment after September 2001, and end with the future, by stating the EDPS role, relating to the EU data protection reform package. Specific attention is

paid to the case law of the Court of Justice and the in their view successful choice of dossiers for EDPS intervention.

The contributions of Louveaux and Laudati focus on the supervision on the EU institutions and bodies. Louveaux gives an overview of how the EDPS has performed his mission of performing and ensuring compliance, and also how he has encouraged a data protection culture. It shows an approach aiming at stimulating accountability, instead of strong enforcement, or in other words using the carrot and not the stick. In the specific context in which the EDPS works, dealing with the public sector, this is an approach which is strongly influenced by the views of Peter Hustinx.

Laudati focuses on a specific area, where very sensitive data are processed on a day to day basis. OLAF, the European anti-fraud office, has been a focus of EDPS-supervision over the last decade, and also here it shows that a cooperative approach using a mix of tools – which does not necessarily mean avoiding the stick – proved to be successful, in order to make officers investigating fraud sensitive to data protection considerations.

A specific and recurring subject in the work of the EDPS has been the relation between public access to documents and data protection. Both were heavily involved in the long discussions in relation to the *Bavarian Lager* case.[11] The EDPS has consistently taken the approach that these two rights are of equal value and that a too stroing focus on data protection may mean that the European institutions could use dat protection as excuse to avoid openness of their decision making processes. In the contribution of Diamandouros this approach is described, and it is also demonstrated that this allow a good cooperation between the EDPS and the European Ombudsman. Diamandouros explains how the latter cooperated with the EDPS, based on a Memorandum of Understanding between the two bodies, and how this was beneficiary to solve cases.

4. How to restore trust?

This book contains contributions of a number of excellent authors, who all discuss different matters relating to privacy and data protection. We hope that their contributions – which include analyses, reflections and suggestions – could be helpful in finding ways to restore trust.

We have qualified the challenge to restore trust as the most emminent one. As stated, in our view, governments have to show that the matter is not growing out of hand and should regain control by ensuring the issue is fully governed by the rule of law.

Governments – and that is even more the case for the EU allegedly having a democratic deficit – base their legitimacy for a big part on the capacity to deliver, and to protect. One of

[11] Case C-28/08 P, see footnote ***.

the main incentives to have the new GDPR into force in the years to come is that it is an important step in getting back control. An important positive consequence of the reform would be the substantially stronger enforcement powers. Also in the US we see tendencies towards regaining trust. This is demonstrated by the Obama paper, and the follow up it will hopefully get through legislation and in any event through enforcement, e.g. by the Federal Trade Commisson, and more in general by all further initiatives aiming at strengthening the instruments for data privacy. Another example is the strengthening of the Privacy and Civil Liberties Oversight Board which could regain trust in the specific context of NSA.

Trust amongst countries should be restored by reaching more global solutions for data protection. Examples are the – renewed - Council of Europe Convention 108 which is open for signature for non EU countries, and the initiative towards UN action in this field. Also, enforcement cooperation should be mentioned.

Trust is also enhanced by increasing transparency. Transparency is one of the essential elements of data protection. One has the right to be informed about processing and to have access to ones personal data (which is also explicitly mentioned in Article 8 of the EU Charter of Fundamental Rights). Effective data protection could also in that sense restore trust.

Against this background, what have we learned from the contributions to this book?

The paradigm of a big brother requires further thinking. What is clear in any event is that the balance of power needs to be restored, in the sense that the overview of what happens in the world of big data should be with democratically controlled institutions, under the rule of law. This does of course not mean that those institutions should become themselves big data controllers, but that they have the overview of what is happening, in order to be able to intervene where this is really needed.

A lot is said in this book on constitutional values: these values help judges, where possible, to give an interpretation to the law which holds pace with current developments. They give guidance to all stakeholders in how to act in this highly dynamic environment with constant, and often fundamental, innovations. In this context, it seems more and more important to distinguish between the value of privacy, the “traditional” fundamental right - with roots in the nineteenth centrury, as this book shows – that needs to be respected, and the claim individuals have that their data are protected, according to transparent rules of the game.

Respect of constitutional values of privacy and data protection also requires a balancing with other protected values, such as transparency and public access to documents, as well as freedom of speech. In this context, the book shows us that in an internet environment, the interactions between those values become more obvious. The growing use of data by governments, and the fact that documents that are made public and should remain public for

good reasons, also affect individuals whose personal data are put in the public domain. Also this is an area that needs further reflection.

Obviously the main balance that needs to be restored, as shown by the NSA case, is the balance between privacy and data protection on the one hand, and security on the other hand. This book shows a number of examples how difficult this is, and shows that this is the recurring issue, over times and circumstances. The main challenge will be to use the NSA-case to make progress in this area.

Moreover, the EU and the US do share basic values. Basic values should be used as the basis to reach agreement which keeps data protection at the right level. Interoperability of legal systems, based on common basic values, could be the start of more global solutions. In fact, this is a way forward that is not much different than the incremental approach which the EU uses to build an area of freedom, security and justice, based on the principle of mutual recognition which presupposes agreement on underlying basic values.

Another area that is touched upon is the relation with competition law. This domain is relatively new and needs further exploration, but it is obvious that the possibility that big internet players become into control of large amounts of data, is a concern for data protection as well as for free competition.

As stated before, the renovation of our legislative system is a huge effort, in the EU where good progress is made, as well as in the US where efforts are huge, but progress less. This new legislation should focus on relatively new elements, such as the principle of acountability. The true solutions that should be found, must be on the scope of application. The difficulty is shown, more concretely, in the NSA-case, where conflicting legal obligations exist on both sides of the Atlantic. The most obvious solution for the authorities of the EU and its Member States would be to enforce EU data protection laws against companies that allow access to their systems, or to strengthen the data protection laws[12]. However, this denies the fact that the main breach of data protection laws is the result of action of a foreign government, not of the choice of an individual company.

Enforcement by regulatory authorities must play an huge role in bridging the gap between the law and paper and application of the law in practice. The central role of the independent data protection authorities in the EU - at national, subnatonal and at Europen level – has been emphasised by the Court of Justice, whereas in the US we see that the Federal Trade Commission is a driving factor in delivering protection. Further strengthening of the roles of all these authorities (at least in the EU) is the first step. A second step is finding new mechanisms for enforcement cooperation, and taking away obstacles, having to do for instance with limitations in sharing (personal) information in investigations.

[12] The proposed Article 43a of the General Data Protection Regulation in the version of the text adopted by the LIBE Committee on 21.10.2013, is a good example.

Using the lessons by Peter Hustinx

In these circumstances, and with these challenges ahead, Peter Hustinx' second term as EDPS comes to an end, marking the end of his impressive career. All authors recognise the wisdom with which he has guided debate on data protection, or as Reding put it his life's work that is bearing fuit and the fingerprint he left behind.

Now, it is the assignment of all of us to continue this work and do our utmost so that control over data and trust can be regained.

In those efforts we should not forget the lessons learnt from Peter Hustinx. What are these lessons?

In the first place, consistency. His views remain consistent, on any issue relating to data protection. Therefore, it is still useful to read earlier opinions of the EDPS, or of the Article 29 Working Party under his chairmanship. They represent views that are still up to date, despite the huge technological developments.

In the second place, pragmatism. Data protection authorities will not be convincing if they overstate the importance of the fundamental right they protect. In the same sense he embraced the famous quote by former UK ICO Richard Thomas: "selective in order to be effective".

In the third place, patience. Some changes will come organically, so we just need to be patient, influencing there were relevant, but avoiding push back. Keep the bigger picture in mind and avoid the uphill battle where possible, but without deviating from consistent views.

In the fourth place, perseverence, availability and hard work. In the EDPS-policy paper on legislative consultation[13] it is stated that the EDPS is available for consultation during the whole process of legislative consultation. That is how we also got to know Peter Hustinx, always available for advice.

We feel honoured that we had the privilege to work Peter Hustinx.

[13] Available at the EDPS website: <https://secure.edps.europa.eu/EDPSWEB/edps/Consultation>.