Jan Philipp Albrecht MEP

HANDS OFF OUR DATA!

The Greens | EFA
in the European Parliament

Jan Philipp Albrecht

Hands off our data!

About the author:

Jan Philipp Albrecht is the spokesperson for Justice and Home Affairs of the Greens/European Free Alliance in the European Parliament. He is the Vice-Chair of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) and a substitute member of the Committee on the Internal Market and Consumer Protection (IMCO). Since March 2012, Jan Philipp Albrecht is the rapporteur of the European Parliament for the general data protection regulation. Jan Philipp Albrecht is also rapporteur for the EU-US data protection umbrella agreement and for the LIBE opinions on the EU-US trade agreement TTIP and the Trade in Services Agreement (TiSA).

He studied law in Bremen, Berlin and Brussels and graduated in information and technology law (LL.M) from the Universities of Hanover and Oslo. Since 1999, Jan Philipp Albrecht has committed himself to the German Green Party in a wide range of contexts. Thanks to his efforts to promote data protection, the former federal spokesman of the Young Greens in Germany (2006 – 2008) has rapidly gained a reputation within the European Parliament as an expert on home affairs, justice and legal affairs.

Jan Philipp Albrecht was born on 20 December 1982 in Braunschweig and represents Northern Germany in the European Parliament.

Jan Philipp Albrecht

HANDS OFF OUR DATA!

English-language edition
first published by Jan Philipp Albrecht 2015

First published as
Finger weg von unseren Daten!
Wie wir entmündigt und ausgenommen werden
© 2014 Knaur Taschenbuch

Jan Philipp Albrecht
Member of the European Parliament
European Parliament · ASP 05F343
Rue Wiertz 60 · B-1047 Brussels
www.janalbrecht.eu
jan.albrecht@europarl.europa.eu
@janalbrecht

ISBN 978-3-00-051 137-0

Layout cover: p*zwei
Layout and Print: AktivDruck Göttingen
set in Adobe Garamond and TheSans
Images: Jan Philipp Albrecht by Fritz Schumann,
Cover: inkje/photocase.de

Contents

»Everyone has the right to the protection of personal data concerning him or her.«

Article 8 (1) Charter of fundamental rights of the European Union

»A social order in which individuals can no longer ascertain who knows what about them would not be compatible with the right to informational self-determination.«

German Constitutional Court on the Census Act, 15 December 1983 (BVerfGE 65, 1)

The great sea-change

Until just a few years ago, the occasions on which personal information about us was stored were rare indeed. Nowadays, this happens almost once a second and involves millions of items of data at a time. Whereas over 400 million people were using the internet back in 2000, that number has risen to over 2.7 billion by 2014, and almost half of those users access the internet using mobile devices. Each month, global data traffic encompasses a mass of around 70 million terabytes. Before the advent of digitalisation, no-one, with the exception of a small number of secret service organisations or registration offices, wanted to go to the trouble of maintaining complicated archives of seemingly never-ending and presumably superfluous information about our everyday lives. Because of the rapid pace of technological advances, particularly affecting storage and network capacities, our lives, confined until recently to the analogue world, have – seemingly overnight – been completely digitised. From browsers to online gaming and smartphones, mostly developed by young IT experts in Silicon Valley, the details behind the new digital technologies have remained beyond the knowledge of the vast majority of people. It was sufficient to be aware that digitisation has happened, and that it supposedly makes our lives so much simpler and happier. For a long time, however, only very few people were aware of the fact that behind these new developments lay a calculated plan, encouraged

by the US government and the US military, to seize power and conquer markets. With that in mind, the portfolio of the CIA investment company, In-Q-Tel, includes technology and internet companies, which, for a large part, follow the state security interests of the USA. This fact was not revealed to the public until the revelation of the NSA scandal in summer 2013. This brought to light a development that had established itself over a period of years and is now completely out of control. The more elaborate the programs became, the less it was possible to maintain an overview of the technology that had been developed, even for those that invented them. Nowadays, the algorithms of search engines and creditworthiness reports are so secret that they are guarded as intensely as the access codes to a bank vault. Even the fate of the global financial market – and therefore of us all – lies in the hands of only a small number of individuals who are still able to comprehend the rules governing decisions taken by intelligent commercial algorithms that are used to organise the automated trading carried out by large-scale investors and banks that, in some cases, is conducted on a high-frequency basis. For years now, lawyers and politicians have been scratching their heads in order to decide, what, given the situation that has arisen, they can actually still do to uphold democratic decisions and constitutional principles. Above all else, this is reflected in the single fundamental rule that governs the streamlined processing of data that we know today: the right to data protection. The conflict between

people, a regulated market economy and democracy on the one hand and machines, multi-national companies and governments on the other is now turning into a battle of superlatives. But how did things get this way? Anyone who wants to understand the history of this burning conflict in the area of data protection must first of all take a closer look at the events that took place during the past 30 years of its existence. The Federal Constitutional Court in Germany developed the concept of informational self-determination in a ruling issued on 15 December 1983 relating to personal information collected during the census. Whilst this concept firstly broke away from the »right to privacy« customarily applied in Anglo-US law, which had been laid down in the preceding years, it is actually much more relevant than the concept of data protection, which is nowadays customary in Germany and Europe. The reason for this lies in the fact that as a concept, informational self-determination relates to an individual human being, whereas the concept of »data protection« is open to the incorrect interpretation that it is all about protecting the data themselves. Historically speaking, however, it was all about the dignity and self-determination of individuals themselves – such as could be achieved by retaining control over information and data specifically relating to them. At the same time, however, this is also the story of two particular developments, the effects of which pervade all areas of our lives: globalisation, which has revolutionised society, and digitalisation, which formed the

technical catalyst behind that revolution. Globalisation was triggered by the opening up of frontiers, the systematic opening up of markets and the advent of a world that is networked in the truest sense of the word. Not only does this inherent drive towards liberalisation give rise to the loss of interrelationships and certainties to which one has become accustomed, but it has also given rise to a historic upsurge of individuals and entire populations as they forge ahead into a future that is of their own making. This has been demonstrated quite clearly by the fall of the Iron Curtain and by the current tensions in Eastern Europe and the Arab nations. Digitalisation came into being following the invention of high-performance computers, data storage interfaces and the development of global communications networks. Thanks to these, we have witnessed a spectacular increase in the number of opportunities open to individuals and entire societies, a fact that is demonstrated equally effectively by the democratisation movements that exist at present, as well as by the new forms of individual organisation that are now available in the private and professional sphere.

The first of these phenomena has given rise to a trend identified a number of years ago by critics of globalisation: the circumvention of existing standards and legal systems. In the first instance, this is manifesting itself in areas such as social and environmental standards and taxation, wherever banks, investors and multina-

tional companies are calling into question any form of regulation as a result of the policies they adopt when selecting their business location and their desire, driven by professional motives, to seek out and uncover loopholes. In fact, globalisation actually imposes an additional challenge to all democratic nations, requiring us to prevent the silent erosion of our systems of law as a result of competitive pressure and actual attempts to circumvent the decisions made by sovereign nations. If, as Europeans, we reflect upon our predominantly negative experiences of the effects and effectiveness of isolation, protectionism and particularism, all that remains for us is to move forward. In the past, all three of these factors have given rise to commercial and political distortions, whilst continually being undermined by loopholes and organised crime. This means that equivalent standards must be put in place on a European and international level – with an uncertain outcome. Whether it will be possible to convince a largely deregulated state such as the USA, or states with repressive governments such as China, of the benefits of equivalent standards governing the protection of our legal principles, is more than questionable. Something that it is impossible to predict is the precise point in time at which such standards could be implemented. For every day that goes by without the existence of common standards, we stand to lose a small piece of these hard-won principles to which we are accustomed.

The second of the phenomena referred to above, namely digitalisation, makes the necessity of a society-driven response in the form of an innovative legal framework on a European and international level even clearer than before. As a result of the abandonment of material factors and the translation of analogue into digital, the existing waypoints demarcating our current state apparatus are almost without meaning: frontiers, the importing and exporting of goods (coupled with the checking or limitation of the same), the location of company headquarters and even territoriality itself. Trading in products is now making way for the trading in data. Ultimately this may lead to something that people still find difficult to conceive, namely the rematerialisation of digitised data using a 3D printer. This, in itself, is the forerunner of a world of science fiction in which it is even within our capability to replicate organs of the human body. Up to now, this particular innovation is still in its early stages, however it is already clear that the range of possibilities that are available to us exceeds our ability to conceive of them, if all that we need in order to produce an identical copy of an object or a human being is the information relating to it. For a number of years now, the concept of identity theft has played a crucial role. Credit cards are copied, and fingerprints and even iris scans used for identification purposes can be stolen with ease. The focus of our economic and social lives is shifting from actions in the real world to digital communication, but what we are neglecting to do is to consider how the

traditional safeguards that operate in a society can be transformed alongside. The analogue is becoming a slave to the digital. Data increasingly determine what happens when, and where. Silicon Valley's answer to this dramatic revolution that is taking place in our societies is to take the attitude that everything will be fine. Nothing can go wrong, because the Googles and Facebooks of this world will take care of us. *We do no harm,* they say, as they disempower us not only as customers who consume what they have to offer, but also as citizens of democratic societies governed by the rule of law. They dictate their rules to us. This is particularly true with regard to those factors that drive and perpetuate their new economy, namely our ›personal data‹, which make it possible to deduce our wishes, our ability to perform, our way of life and our weaknesses. They collect whatever information they are able to obtain about us. This is done without asking for our permission and without even providing us with any detailed information. The hard currency of the digital age is, as it were, being filched out of our pockets without our even noticing. This process has been going on so surreptitiously and, for all practical purposes, without regulation that the businesses we have hitherto regarded as insignificant websites are now the biggest undertakings in the world. They have greater scope for action and more influence than virtually any business or state in history. If things remain as they are, we shall be completely disenfranchised and easily fleeced in the digitised world. We shall find ourselves living in a to-

talitarian controlled society, which has only been able to come into existence and to hold sway thanks to the masses of information gathered about us, and which is becoming daily more entrenched by the same means.

It is one of the most serious derelictions of duty in history that political decision-makers ignored this development for so many years. It is true that the history of data protection and the regulation of information technology is marked by legal milestones that have been erected on various occasions, but the true dimensions of the problem have never been correctly recognised by politicians, judicial authorities, the media, businesses or most of civil society. Despite the surveillance scandals of the past and numerous clearly perceptible aberrations in the approach to personal data, data protection has again and again been regarded as a peripheral, technical matter and as a low priority politically. In a survey carried out in January 2014 by the German television channel ZDF into the most significant challenges that lay before us in the political sphere, data protection only appeared in 15th place, having been identified by only 3 percent of those questioned. And this, despite the fact that it is the only fundamental rule that plays a central role in the digitised lives we lead. The exercising of fundamental rights, the development of democracy, compliance with the laws of the State and the implementation of current and future regulations will depend upon whether the liberal, democratic states of the world and, first and foremost, Europe, are

able to guarantee the effective protection of our informational self-determination – that is, our freedom to make decisions and our control of our own identity – even in the globalised and digital age in which we live. We must once again become the masters in our own domain and be able to decide freely, which items of information we wish to reveal and in what situations. The purpose of the publication is to record the challenges that stand in the way of this freedom and to state what must happen in order that this freedom can continue to be guaranteed in the future. Using a number of examples, I would like to show you why data protection has the power to determine the course of all of our lives and to point out the dangers we will face if we are unable to find any effective rules that can be used in order to govern it. The purpose of this book is to raise awareness and to provide a wake-up call, as in the absence of a social upheaval that will lead us into a future characterised by self-determination in the digital age, we will be unable to conquer the major challenges facing one of our most important fundamental rights and the underlying human virtue it sets out to uphold.

What is the purpose of data protection anyway?

Many people ask me, »what is the actual purpose of data protection?« And a great many of them say to me: That whole business about data protection isn't that important to me, but I think it's a good thing that you are concerned about it. Though I am glad to accept the confidence those people have placed in me, those types of statements always make me cringe. To me, they sound is if someone is actually saying: I don't really care, whether we make our way through our lives in a way that provides us with self-determination and upholds our dignity as human beings. But it is great that you actually care about this unimportant issue. What many people do not notice, however, is that the fundamental issue underlying data protection affects them every single day of their lives, namely what information about me as an individual should be made known to whom and in what situations? If I am not in a position to decide that for myself, I will also lose the ability to exert control and influence in relation to other issues. Since time immemorial, the ability of an individual to divulge specific information or keep it to himself has played a decisive role that has affected the survival and continued existence of an individual. This began back in the Stone Age, when it was necessary not to make others aware of our physical weaknesses, was for many centuries associated with the crucial, life-or-death issue regarding our religious affiliation and now-

adays finds its counterpart in the form of information relating to our purchasing power. Nowadays, anyone applying for a job is not only put through their professional paces, but their social life, private predilections and social risk factors are scrutinised in great detail as well. Situations are even alleged to have arisen, in which potential employers have not merely viewed the information available on a candidate's public profile on social networking sites, but have required job applicants to divulge the password for their own account. Only those who granted access to their own news feed and, in some cases, intimate details, would then be considered for appointment.

Nowadays, anyone who, like many millions of others, exclusively makes use of the internet as a means of partaking of services, is automatically surveyed by insurance companies, banks and information agencies for factors that may point to the possibility that we may default on a payment. Without even noticing it, customers with different levels of disposable income are shown different offers and means of payment. Even the prices may be different in each case, depending on the way in which the information that is available is evaluated. For example, the *Wall Street Journal* revealed in the summer of 2012, that the online travel portal, »Orbitz«, initially displayed higher prices to Apple users than it did to Windows users. Based upon user analyses, Orbitz had come to the conclusion that customers using Apple products are generally prepared to

spend more money than customers using Windows devices. As a result of the increasing availability of personal data and the increasing precision of automated analytical processes, the evaluation of individual human beings is set to become the latest factor that is used to distinguish one person from another within our society. Whereas in the past, the fact that an individual belonged to a clan, to the nobility or to the upper classes of society played a decisive role in determining the opportunities that came his or her way within society and in the commercial domain, the analysis of big data using score-values (a figure, which, by means of a calculation, is meant to represent factors such as a customer's ability to pay) is now taking on the task of separating the wheat from the chaff. But this is not happening in a general way, but in each individual stage of life, commencing in pre-school education, continuing during an individual's school education and vocational training through to the time at which he or she finds his/her first job and makes use of the opportunities for self-realisation that are on offer in the world of today. Each individual item of information that is known about us can have an enduring effect on our entire life. What time did our internet-enabled smartphone alarm wake us up this morning? How much water consumption and use of our central heating system was recorded by means of the smart metering system, which enables the energy needs of our home to be recorded and analysed down to the second? What route did we take to work and during the day in the company of our smartphone that is always within

reach of WiFi networks, or in our car that makes use of GPS navigation? How fast did we drive between one toll booth and the next? Whom did we call or with whom did we exchange messages? How often, when and for how long do we surf on which particular websites? Which books and magazines do we buy? In no time at all, and without even knowing our name, these items of information alone would be sufficient to draw up a comprehensive personal profile, which, in a world that is home to 7 billion people, would be specific to us alone. That profile would say more about us than we would necessarily tell even our closest friends. Anyone who manages to get hold of that information would have the potential to turn our life completely upside down, from one day to the next. Whereas in the past, it would only rarely have been worth the effort to search through the life of another person in search of inconsistencies and abnormalities, this has now become a service that is available at a cost of only a few euros. The demand for this type of individual customer analysis is enormous. Many companies in the mail order, insurance and banking sectors actually make use of these services at the time that a customer shows any interest whatsoever in a product. The profile or score value of the interested customer can be accessed in just a few seconds. The growth potential for data analysis is expanding beyond all limitation. Any company that is active in big data will be big business tomorrow. What is more, we are no longer the customers, but the commodities.

Many people are unaware that data protection forms an inseparable core component of our dignity as human beings and of all of our civic freedoms available within a free and constitutional democracy. It will not be possible for us to exercise any of our fundamental rights, if we have lost control of our own identity and of our personal information. For example, we are free to take part in demonstrations; if, however, I must expect that information regarding my participation in demonstrations will automatically be recorded and made available to insurers, employers or the authorities, my free decision to exercise my fundamental right has been severely limited. At the same time, this limitation not only curtails the freedoms available to us as individuals, but also constitutes a threat to democracy. After all, it is the opinions expressed by individuals of a different persuasion that actually enable an active democracy to operate. If, however, our freedom of information is restricted, due to the fear that by entering certain search terms into online encyclopaedias or by lending out relevant books – which actually occurs – would lead to significant consequences, such as our arrest or deportation, the extent to which our democratic civil society is operating effectively will decrease rapidly. The increasingly comprehensive retention and processing of information dramatically increases the likelihood that this will give rise to negative consequences upon our lives as a whole. For example, if an evaluation of the likelihood that I will suffer illness is based upon the fact that I regularly purchase an un-

healthy amount of sweets, or if my employer makes me redundant due to the fact that the attitude I adopt in my private life would be detrimental to the company's image.

Or, let's take our right to freedom of opinion as another example: Anyone who anticipates that merely expressing his or her opinion will lead to a complete examination of their entire life or that any opinions they express will automatically continue to affect them in all aspects of life will refrain from expressing any opinions at all. And anyone who expects that the authorities will always get to know about an opinion expressed in private or within an intimate group, as a result of eavesdropping upon conversations by cleverly tapping into the microphones of the smartphones present in the room, will quickly adapt his or her behaviour. What is more, the limits of our professional and religious freedom may very soon be reached, if constant observation and data retention create a situation, in which mundane items of information about our lives enable others to draw inferences with regard to what religion, trade union or party we belong to. The way in which individuals can prevent any evaluations from being made about them, based upon other information, is by keeping certain items of personal information (especially intimate ones) to themselves. Nowadays, no-one can hold secrets or private predilections any more, without others being able to work them out or at least surmise them to a high degree of

probability. Whether these relate to our private love interest, the fact that we attend Alcoholics Anonymous, are colour-blind or our favourite spot in the park – all of our individual predilections and behaviour patterns can nowadays be stored in the form of metadata, which enable others to predict these aspects with a fairly high degree of probability. Anyone who wishes to determine his or her own life and preserve his or her privacy is now obliged to regain control over the ways in which such metadata are distributed and to erase his or her traces, or at least anonymise them.

Data protection is all about protecting people and their right to self-determination. The rules should not be about protecting the data themselves, but protecting individuals' right to self-determination. In order to preserve this, it will take much more than a simple statement of intent, specifying that the information will not be »abused« or used for any purpose for which it was not intended. That is why we need to have control over all of our information, but that is no longer possible nowadays. Contrary to what most people think and are led to believe by relevant parties, we lost control over our personal data a long time ago. In the vast majority of cases, data are processed without the knowledge or consent of the person concerned. The primary reason for this is that individuals are unaware of the types of individual data processing that take place. The processes that take place inside our computers, smartphones and tablets, together with the

many networked devices that now exist, are totally unknown to us. We do not have any conception as to how many electrons and items of data are wafting through the circuits, where they are directed to, or where they mistakenly end up. We are exposed to the mercies of an invisible world of high-tech processes designed by information technologists and IT companies. In order to change this situation and put ourselves back in the driving seat, we need data processing regulations that will form a foundation for the society in which we live. Data protection law would then encompass the fundamental rules for the terms and conditions of our own being and actions. As individuals. Without the ability to determine the way in which information about us is processed, we will become beings that are governed by third parties and whose behaviour and actions can simply be predicted by calculation. For example, it will be possible to determine, with almost absolute certainty, what we will do next, what needs and problems we have, what our health and performance are like and what behavioural patterns we are displaying. Nowadays, as soon as any irregularity is detected in our profile or as soon as the details no longer correspond to one another, this is frequently sufficient to trigger an alarm signal. That alarm is intended to draw attention to the fact that something is not correct or is no longer in keeping with the relevant predictable patterns and calculations. In many cases, this is then regarded as a danger to the organisation that is collecting the data, whether that is a private company, the state

or society itself. Dystopias, such as those encountered in works such as George Orwell's »1984«, in the film »Minority Report« or the novel »The Circle« by David Eggers, illustrate the extent to which the power that can be obtained as a result of the processing of data can be abused. »Knowledge is power«, says a well-known proverb. And it becomes even more powerful, if that knowledge relates to other people, as it is no longer restricted to our ability to shape nature, but enables us to affect the population as a whole, in the form of each individual person. And the fact that the details concerning our lives are converted into digital format as a matter of course mean that it is extremely easy to evaluate them quickly, cheaply and extensively. That is why data protection is one of the most essential rules that exist in this digital age. Data protection determines precisely who is permitted to evaluate what quantity of information about us and for what purpose.

When, in 1983, the German Constitutional Court handed down its groundbreaking ruling in the case involving the census data, citing the fundamental right to informational self-determination that forms part of the German Basic Law, the protection of privacy and data protection had already formed the subject of disputes for several decades. After a debate regarding the registration of US citizens got underway in the USA in the 1960s, it also made its presence felt far away in the German federal state of Hesse, which at that time was home to large numbers of American forces personnel.

A discussion about data protection and the estimation of the consequences of technological development ultimately led to the adoption of the world's first data protection legislation in 1970. When, a short time later, a body of legislation was created in the USA in order to prevent random incursions into the privacy of individuals (i.e. unlawful incursions or those not ordered by a court of law), the signs were already there that Europe and America would diverge in this area. For example, the Privacy Act of 1974 set out to protect the privacy of US citizens against the authorities of state, whilst the political initiatives in Europe were dominated by the concept of »data protection« and set out to protect all individuals against any party involved in the processing of personal data. Whilst the debate in the US regarding the »Right to privacy« continued to focus upon the right of the individual to be protected against the State, what developed in Europe took the form of dogma in which data protection formed a task for the government to provide protection that would apply to all forms of data processing and the consequences of these for individuals and society. That development was not without reason. In many parts of Europe, not only in Germany, the experiences of domination by a foreign power, dictatorship and surveillance were still ever-present or even formed a current issue. The realisation that each instance of data processing could have severe consequences for the individuals affected was an issue that dominated the minds of scientists, politicians and civil rights activists alike.

You may well recall that civil registration systems and punchcard systems, amongst other things, helped the Nazis to achieve the large-scale detection and destruction of Jews throughout Europe. Maybe they had already recognised the effects that the increase in processing of personal data, relating, for example, to trade union membership or religious affiliation, had upon minorities the world over. And perhaps they had a more clear conception as to the effects that continual checking of the most banal types of information would have upon individuals' freedom of action in countries such as the German Democratic Republic (GDR). The German Constitutional Court then handed down a memorable ruling, stating that data protection did not arise by virtue of the secrecy of telecommunications or the protection of property (in other words, one's own four walls), but from Articles 1 and 2 of the Basic Law of the Federal Republic of Germany. Informational self-determination formed an expression of the most important principle underlying the German Constitution – the principle of human dignity – and of our fundamental right to protect our own identity. The ruling of the Court therefore stated clearly that any action capable of restricting the informational self-determination of an individual had the potential to constitute an incursion into his or her fundamental rights. In its ruling, the Court set out to emphasise firmly that it did not matter, whether any such incursion was carried out by State bodies or private parties. Any process that handles information relating to an individual may represent a threat to his/her dignity

and personal rights. In view of what has already been said with regard to the current situation, it is worth noting that the German Constitutional Court came to these conclusions as long ago as 1983, at a time when the far-reaching and comprehensive data-processing facilities we know today were still a long way off. In handing down its ruling, the Court exercised a significant influence upon the subsequent development and dissemination of data protection law in Europe and throughout the world.

This far-sighted ruling by the Constitutional Court also contained an important statement that had no further repercussions, namely that the concept of data protection actually does not relate to the very things that are supposed to be protected. It is actually not the data that enjoy the protection of an important fundamental right, but individual citizens and their right to self-determination. In that regard, the concept of informational self-determination was a forward-looking and multi-faceted creation. Especially since it clearly set out to distinguish itself from the »right to privacy« approach adopted in the USA and set out to ensure comprehensive protection of the right to self-determination in all spheres of life. Unfortunately, as is often true of terms created by the Federal Constitutional Court, the concept was not sufficiently understandable to the population at large. As a result, the concept of »data protection« established itself as a familiar concept, although it is still affected by the misconception with regard to exactly what it sets out to protect.

Contrary to what has been said in certain arenas, data protection is therefore not simply a reaction to innovative demands in the area of consumer protection. It actually arises from two important human rights, namely general personal rights and the right to human dignity. Not only do these set out to uphold a standard with regard to individual freedom and the right to be protected, but they also require the State to fulfil the task of protecting its citizens. With regard to individual dignity, this even exists to such a degree that in certain cases, even the individual concerned cannot even do away with the protections afforded to him/her under the Constitution. For example, the consequences with regard to informational self-determination would be severe, in the event that all individuals were to reveal all of the information relating to themselves. In that instance, it would be almost impossible, as an individual, to arrive at a free decision regarding whether or not to reveal information of a personal nature. Any decision not to make public such information would then be regarded with equal severity as an admission of a substantial weakness. This would then result in all disadvantages and specific attributes being made public, irrespective of whether these were relevant or of any ethical criteria and would constitute an open door to discrimination. What this tells us is that even our right to equality is closely connected with effective data protection. Only if every single one of us is equally able to exercise his or her fundamental rights, can those fundamental rights be applied to us all. Anyone who finds

themselves in a position, in which he/she is no longer freely able to exercise his/her fundamental rights, is no longer able to play an equal part in the life of society. The principle of equality, or the prohibition of discrimination, is firmly embedded in both the German Basic Law and in the Treaties enacted by the European Union. The concept of »Big Data« that we know today calls this principle into question in a fundamental way. If used to process personal data, the profiling and data mining technology underlying the concept of big data is, in itself, a method of discrimination and not, as many people like to suggest, an improved or more advanced form of science that will only be of benefit to all concerned. The creation of more comprehensive and increasingly accurate personal profiles actually does away with any guarantee of equality, due to the fact that such profiles provide too many items of information that may be used for the purpose of »justified« inequality of treatment. Do we really want to find ourselves in a situation, in which we will be asked to answer the following questions: Is it appropriate that a person who leads an unhealthy lifestyle receives the same level of healthcare as someone who maintains a healthy lifestyle? Should the parents of children whose achievement at school is poor receive fewer social benefits? If organisations such as the state pension and health insurance bodies and employment agencies set out to record data, it is likely that this trend will be on the increase. Companies may ask themselves: Would it not be useful to make different offers to different peo-

ple, therefore not simply offering different products, depending on an individual's interests, but a different range of services and prices?

The International Air Transport Association (IATA) is already considering a scenario in which anyone searching for flights on the internet will be required to log in first. Websites such as Opodo, Swoodoo or Expedia would then be obliged to record our personal details, before we were even allowed to search for a flight. The idea behind this is a very simple one: you provide the customer with offers, based on the type of person carrying out the search. A businesswoman who is relying on being able to take a specific flight at short notice, would possibly then be required to pay a significantly higher price than a person making a last-minute booking in order to travel to a holiday destination, even though both people would be making use of the same type of ticket. Although such inequalities would, in many cases, be against the law, the consumer organisations and authorities are already powerless to intervene. The use of complex, invisible algorithms means that it will become impossible to check the many millions of processes involving the tiniest pieces of metadata in order to detect any unjustified discrimination. And even if forward-looking thinkers such as Viktor Mayer-Schönberger, an Austrian and a Professor at Oxford University, are predicting that in the future, algorithmists will fulfil a similar role within society to the one played by law-

yers at the moment, the necessary element of self-determination will continue to be crucially important.

A free society and a free market economy can only operate, if they are fundamentally based upon the equality of regulations and equality of status between all participants. One of the tasks of a democratic political system is to guarantee that equality and to identify any situations that do not uphold that equality and, if necessary, justify them or reduce them. The power exerted by information processing makes this difficult, however, as the inequality that exists between the various parties involved is not clear for all to see. Information processing regularly takes place unseen, just like any thoughts we may have about the other party cannot be read (for the moment, at least, until such time as the latest advances in neurosciences, in which electrodes can be connected to the brain, in order to enable artificial ears or eyes to be used). The greater the difference in the level of knowledge held by two individuals (whether in a natural, legal or technical form), the more unequal are their positions. The best example for this is Google. Users of Google's service see an almost empty webpage displaying the Google logo, with its friendly and jolly appearance, and a single input form. By entering key words, the site magically provides suitable results from the billions of pages on the world wide web. No explanation is provided as to how this actually works, nor does any display appear, showing the information that is being collected about the users. For its own part, the Google company,

which, according to information it has provided, is one of the largest companies in the world and exerts more influence than many countries, has built up a deep insight into the lives and characteristics of its users. This is not limited to information about their location, the browser they are using, their search habits or their ability to use certain languages, but also includes the complete history of every term they have ever searched for and any pages they have viewed. All of that information is then used for computational purposes and is associated with millions and millions of other items of information. To Google, knowing our real name is something that is of secondary importance. The key issue is who Google believes us to be, based upon characteristics such as our purchasing habits, our ability to pay, our social environment, our visions of life, our political and religious opinions, our sexual orientation, our state of health, our future prospects, our job, our hobbies, our predilections and so on. In other words: everything! After all, these are the intimate details that make up our entire lives and personality and which enable inferences to be drawn about all facts that relate to us. In view of the masses of information about us that has been collected on a daily basis over the years, Google's records database is much less prone to fraud than that of any municipal register. There's no way we can pull the wool over Google's eyes, nor should we be under any illusion: we are completely at the mercy of Google.

In Europe, Google has maintained a market share of over 90 percent for a number of years now. Every one of us has helped Google achieve its position of dominance, by providing it with additional data about ourselves and our environment, day in, day out. The majority of us simply have no idea what data are actually involved and what actually happens to them. And almost no-one knows that Google is improving its system on a daily basis. Yes, every single one of us is a voluntary employee of Google, every time we use one of Google's services. Its algorithms are trained to learn from us automatically and to analyse every click and every word we enter in order to improve Google's system. This is a form of artificial intelligence that is becoming ever more opaque and uncontrollable, even for the very programmers that are working on it. As time goes by, Google is turning into a gateway to the world. It exerts greater power over our lives than many nation states or presumed rulers. And it certainly makes use of that power. Highly effectively, but largely unseen, Google and Silicon Valley as a whole are bringing about a greater degree of change to our world than a good many international decisions and laws are capable of doing. Just as remarkable as this threat to democracy is the agenda that lies behind these changes. To find out more, it is worth reading the book by Eric Schmidt, the Executive Chairman of Google, and Jared Cohen, the Director of Google Ideas, which has the revealing title *The New Digital Age. Reshaping the Future of People, Nations and Business.* Google and

its managers are setting out to do nothing less than completely revamp our society in line with the principle of total transparency of human beings and human life itself. In August 2010 at the Technonomy Conference in California, Eric Schmidt said that anonymity is »dangerous«. A month later, in an interview with the *Frankfurter Allgemeine Zeitung*, he went on to say that »openness is my religion«. Following the publications by the NSA whistleblower Edward Snowden, he subsequently appended his previous statements, adding that in the future, privacy would be an anomaly, which individuals would be required to forego.

The interesting thing about all this is the fact that Google itself takes steps to ensure that its own company is itself the greatest secret that has ever existed in economic life. The algorithms used by its services are the best-protected items of information in the world. Instead of stating in public what the company's own interests are, it lends financial support to a highly varied range of diverse social initiatives, scientists, law firms, parties and associations. Of course, all such support is provided without obligation, its only duty being to promote the benefit of human kind. And bit by bit, it is becoming apparent that data protection is being used to serve one predominant purpose: to control the power of those who covertly set out to extend their market domination and economic success, to our detriment and to that of their competitors. Our own self-determination is the most potent weapon that we

can wield in the face of the power exercised by mega-companies and governments alike. The battle around data protection is the final battle in defence of our freedom.

The end of self-determination

The first stages of internet-based communication largely succeeded without making use of any personal data. In many cases, data were only processed in the form of an IP number or mailbox address at the point that a webpage was retrieved or a message was sent. It was not until the advent of the first e-commerce websites and the login systems used by Yahoo!, Facebook and others that there was a massive increase in the processing of personal data. First of all, additional details, such as individuals' address and bank account details, were transferred from the analogue into the digital world. Online services made and still make it easy for users to provide their details. As individuals, we are quick to place significant trust in the fact that the information we submit will be processed securely. In fact, we do so much too quickly. Today, we have reached the point at which Google Glass and the smart car, the networked house and the electronic health check via our smartphone are about to be rolled out to the mass market. Coupled with all manner of information taken from our everyday lives and relating to our individual settings, we are already able to use our glasses or a car that is linked to our systems at home to turn up the heating or to check whether we have any beer at home. The possible applications have increased enormously, but do we still have control over what happens behind the screen or inside these smart devices? Do we really know what types of information our fridge is actually

transmitting, whenever it connects to the »Internet of Things«, which is the very latest trend in networking?

For the burgeoning companies in Silicon Valley, one thing was clear from the outset: the data of its users form the oil that lubricates the digital revolution, and users would associate themselves with the sources that generate that data, as long as they could be obtained cheaply. Companies such as Facebook, Google, Amazon and others are the oil magnates of today and their sources are generating billions of dollars in revenue on an annual basis. As a result, personal data is bursting out of the systems made available by these providers and is happily bought by clients from all sectors of the economy, government and the media. Every one of these is now dependent on data provided by sources located in Silicon Valley. The fact that we have long since reached the point of digital spillover, in which increasing quantities of data about us are draining off in all directions, is a closely guarded secret. Something that has gone entirely unnoticed is the fact that the privatisation of data analysis is the equivalent of the oil catastrophe of the digital age. Whilst some companies are earning more than a small fortune from these brimming sources of oil, increasingly large numbers of people are falling victim to the consequences of this billion-dollar industry – either as a result of identity theft, false scores or discrimination based upon the ruthless outcomes of big data that are difficult to control.

Those victims are consumers, who, once upon a time, showed the red card to the oil companies and took action to protect the environment. The power of the people to vote with their feet and, as consumers, to turn their backs on companies was stronger than the power of governments to get a grip on the consequences caused by uncontrolled profit-seeking. State regulation did not ensue until the people brought their collective power to bear. That situation is exactly the same as the one that we are witnessing today with regard to the processing of personal data. First of all, there was the discovery of the extent of the damage caused by uncontrolled data collection, which set a great many people thinking. The revelations by Edward Snowden regarding the mass storage and analysis of details relating to our everyday lives by the secret services and their agents within the internet companies only served to demonstrate to us all how far things have already developed and how little regulation or effective control the people and society are able to muster.

At that point, we had reached the very core of data protection, as our very self-determination was at stake. As a consumer, I must be in a position in which I am fundamentally able to decide for myself, whether I wish to reveal information about myself, or would rather keep it to myself. Not everyone will actually avail themselves of that right and there will certainly be some who are happy for these matters to be dealt with by third parties and only wish to fulfil their roles as consumers, with as few issues or questions as pos-

sible. But anyone who is not given any point of approach that enables self-determination or receives no opportunity to intervene in the processing of his/her personal data, is being robbed of his/her self-determination and the ability to control his/her identity. At a time in which an individual's identity and profile are now more important than ever before, this would constitute a loss of control over one's own life. More frightening still is the fact that in practice, hardly any situations remain in which we still have any involvement in determining »whether« or »how« our personal details are to be processed. In the vast majority of cases, the companies we do business with simply take our details and either do not inform us of this, or do so in a veiled manner in the small print at the bottom of an application or a webpage, or within completely incomprehensible terms and conditions of business or data protection consisting of several pages of text. Only in very few cases does a company elicit our explicit consent to allow our personal details to be used by other parties. On the one hand, the reason for this is due to the sheer quantity of data that needs to be gathered about us in this day and age. In this regard, we should actually ask ourselves whether we wish to make available such a mass of information or whether we should demand services and offers that do not require such a large quantity of data about us to be processed. On the other hand, a further reason why companies do not explicitly request our consent is because they have established that in many cases, we simply do not wish

to reveal our details. And as they are therefore unable to associate each contract and each offer with a duty to disclose endless quantities of data for completely different purposes, they simply no longer request our consent. In the negotiations relating to the EU data protection reform (a topic to which I will return later), direct marketing companies reproached me about the fact that whenever consent is requested, only 20 percent of individuals would actively give consent for their details to be used for advertising and marketing purposes, whilst 80 percent simply ignore the request. Furthermore, only a further 20 percent would actively withhold consent for their details to be processed, if, in the first instance, they were not asked for their consent, but were simply informed in passing of their right of objection. This would lead us to the conclusion that 60 percent of people actually have no problem with the processing of their personal details, but wouldn't go as far as actually ticking the box on the form. As far as those marketing companies are concerned, the need to request the prior consent of individuals is too severe a burden (and one upon which »thousands of jobs« and the »future of the sector« depend). Understood? In simple terms, these companies wish to make clear that if we have to ask you, whether you want to let us have your details, then it may well be that you don't say anything at all! So please allow us simply to take your details, without having to ask first.

Unfortunately, however, too many companies have already obtained permission from the legislature to do exactly this. As far as direct marketing and online tracking are concerned, a majority of members of Parliament have consistently voted not to grant us the facility to be able to determine in advance, whether our details may be collected and used by another person.

In order to be able to exercise such a decision giving approval (known as »opt-in«) or disapproval (known as »opt-out«) whenever data is being collected and thereby avail ourselves of our right to informational self-determination within the relationship between consumer and company, what is also required is a right to receive information, to request deletion and to be involved in the decision regarding data processing. In the digital world of today and tomorrow, these rights form the most important prerequisite that will enable individuals to enjoy a more effective degree of self-determination in their capacity as responsible citizens and consumers. The fact that the increasing complexity of the data processes that exist nowadays means that it is more difficult for individuals to check and control them makes the need to enact rules to protect the self-determination of the individuals involved even more urgent. This having been said, the power structure is shifting further in favour of the data processor. and that situation is being ruthlessly exploited by the internet companies. Due to the sheer quantity of information provided, they are creating a situation in which

their users are becoming dependent upon their services, which are mostly offered free of charge. Whilst consumers do not expect that their details are being processed, the fact that they make use of the services means that their personal details form part of the way in which they are being exploited, a fact which I will return to in more detail later. The technical applications of the digital world have penetrated all spheres of life and create an impression that they are simply making everything easier. One of the consequences of this is that the linear process of conventional commercial transactions is now a thing of the past: The product is manufactured, sold to the public and then used. That was how things were in the old world. In the meantime, the formula of supply and demand has long since become a more complex process: while production is underway, the first evaluations from customers or users or the first reports of faults are already coming in. These are used in order to optimise the product. And the same thing happens in all of the subsequent stages. At the centre of this new industrial age is the individualised production of goods and services. We are living in a world that is increasingly tailor-made to our own individual needs. But who exactly are the tailors? Who actually produces those goods and services and what criteria do they use to decide how we should conduct our everyday lives?

Changes in the economic process mean that we are also losing the points of orientation provided by a 100-year-old process of civil law. Civil law is based upon

the fact that contractual partners enjoy the fundamental freedom of decision-making and are in possession of the relevant information. At the same time, civil law is also based upon the fact that the conclusion of a contract is a process that is transparent for both parties. Given the increasing complexity of the data algorithms employed, this is, however, much more rarely the case or is even impossible. This asymmetric nature of knowledge is giving rise to a creeping disempowerment of individuals who take up offers or make use of systems. One of the ways in which they are paying for what they receive is by surrendering their influence and sovereignty, causing them to become the plaything of a power over which they have no control. A power that will not hesitate to take them to the cleaners, thereby consigning the autonomy of individuals and with it, the autonomy that we all enjoy within the free market economy and our right of self-determination within a democratic state, to the history books. Against that background, the structures of society however have remained the same, but are being legally undercut as a result of this development.

Not only is our individual right of self-determination disappearing, but the collective right of self-determination held by the democratic sovereign is being lost as well. Put these two things together and what results will be a dangerous and explosive mix, in which populism, conspiracy theories and disenchantment will quickly take hold. The dangerous consequences of unimpeded globalisation are being consistently underes-

timated by politicians, whose focus lies upon achieving short-term success. What is more, the economic and financial crises of our times are the result of a lack of political supervision of the processes of globalisation, and as the digital revolution progresses, those consequences are set to become even more severe. Instead of insisting that the law be applied clearly within their markets, the states of the world have imposed too few binding conditions before parties can gain access to their digital markets. For a number years now, politicians have given companies, especially the major IT companies in Silicon Valley, the impression that it is basically sufficient to adhere to the rules that apply in their region of origin and, if accused of any contravention, to enter into negotiations. The disputes that exist between data protection authorities in Europe and companies such as Google and Facebook enabled us to recognise that the companies were under a fundamental misunderstanding: namely that it was not those companies that had to stick to the rules that apply on a local level, but that their local agents should yield to the »reasonable« considerations of those companies themselves. This particular belief arises from US law, which does not impose any rules upon companies regarding the processing of personal information. In the USA, the handling of our personal information is governed solely by the very vague rules of fair competition and by considerations regarding the image of the company that will be created amongst consumers themselves. Companies such as Facebook and Google do not regard the data

protection authorities in Europe as authorities tasked with implementing and upholding the law, but purely as consumer rights organisations, to which it is simply a case of explaining how things are to be.

What is more, politicians within the EU Member States have clearly failed, as yet, to recognise the fact that as a result of the creation of the common internal market, any company can choose in which EU Member State to establish itself and therefore also, which of the 28 different legal systems of the EU Member States it wishes to abide by. In the case of companies with historical roots or production facilities tied to a particular locality, this clarification brings nothing new. In the case of companies in the digital sector, however, this means the world. All they need in order to establish a suitable head office is a mailbox and internet access. In the meantime, those IT boffins have become established in all parts of Europe and are capable of working anywhere, given sufficient payment. One of the consequences of this situation brought about by the internet companies is that in principle, they select whichever legal system in the EU offers them the best working conditions. It goes without saying that this particular benefit will primarily be of use to those who are neither obliged to set up a new company nor tied to a particular locality. How can that happen, you may ask yourself? It's very simple: as a large company, they enter the EU's internal market, in search of a headquarters inside the EU. In that case, they not only have a free choice as to which legal system and which data

protection obligations they wish to adhere to, but they are also able to hold discussions with individual EU Member States as to how keen those Member States are to welcome them and the many jobs they will bring to each country. There is certainly no better position to be in than this, and during the past 10 to 15 years, a great many companies – especially from the USA – have ruthlessly exploited this beneficial situation, not only in connection with data protection, but also in relation to taxation, environmental standards and consumer standards.

In the case of data protection, however, the loss of government sovereignty is particular high, as the companies involved are internet companies, whose position is a particularly strong one. A blatant example of this type of situation is the one involving Facebook and the Republic of Ireland. Thanks to a neo-liberal dumping policy, Ireland was seeking to inject new life into its ailing economy and so created the most beneficial conditions for IT companies wishing to establish business operations in the country. For Facebook, this formed an opportunity to develop a site located inside the European internal market that would benefit from considerably favourable conditions. The absolutely ideal conditions that the company negotiated in Ireland turned out to be so good for Facebook that the company made its site in Ireland into its Group headquarters for all of its business outside of North America. In other words: the only locations for which

Facebook Ireland is not responsible are the USA and Canada. For the billions of people around the world who nowadays make use of Facebook, this means that if they have a problem, they can only seek assistance from the company's offices in Ireland. It also means that the Irish supervisory authority for data protection has the task of pursuing people's rights again the company. That authority, which fulfils tasks extending across the world, is located on the outskirts of Dublin in an unassuming building above a small supermarket – it is really very small indeed. It became known, however, when, in 2011, a young Austrian by the name of Max Schrems decided to pursue his data protection rights against Facebook. He submitted a data request, requiring Facebook to inform him what data the company held about him. As a Facebook user, he entered and shared information, and exchanged messages. For months on end, nothing further happened. Schrems did not receive any reply. He remained persistent, however and sent renewed requests to Facebook and to the data protection authority in Ireland. Only after the activities of the young student received public attention did things begin to move forward. One day, Schrems received a DVD containing 1222 documents in A4 format, containing a list of all of the personal data about him that Facebook had collected over the years. While he was painstakingly working his way through this massive pile of information, checking it for inaccuracies, he noticed hundreds of instances that infringed data protection legislation, involving details

that he had long since »deleted«. These also included a whole host of information about him and his life that he had never divulged to Facebook. He decided to stand up for his rights by complaining to the Irish data protection authority. Once again, his experience was that the authority remained inactive for a period of months, or initiated discussions with Facebook that ended with reassurances from the company that everything was in order and that this student from Austria was the only one to have complained about things that seem to be of no consequences to all of the other users of its service. It was not until Max Schrems graduated from university that he decided to initiate court proceedings before the competent court, in Dublin, if need be. He managed to scrape together 100,000 euros from donations that enabled him to pay the fees of a lawyer in Ireland and the cost of the legal proceedings themselves. Ultimately, the case could cost up to 300,000 euros, if the proceedings dragged on, as they were expected to do. Only after having reached the end of those proceedings, would he be able to bring the case before the European Court of Justice in Luxembourg. Anyone who is interested can follow his ongoing battle with Facebook, which began in 2011, regarding the alleged 23 infringements of data protection law by visiting the website of the association Europe vs. Facebook, which Schrems himself set up. The site contains a chronology of charting the disempowerment of consumers in the EU by a company that has cosied up to a data protection authority and a legal system that is not

implementing and upholding the existing data protection rights within the EU. This constitutes a breach of EU regulations.

The example of Max Schrems demonstrates only too clearly that the battle for the protection of our data was lost a long time ago. Using the rules governing free trade, companies are able to make use of *Forum Shopping,* which gives them the opportunity to select whichever system of law or location within the European or international market that provides the rules that most closely suit their purposes for each and every transaction, so as to circumvent the legal stipulations that we have come to expect and to play them off against one another. The distance that lies between the company headquarters and the consumers additionally makes it more difficult for critical consumers or private individuals to submit uncomfortable enquiries, with the result that they do so less frequently. With regard to objections or even complaints, this even creates a situation in which it becomes almost impossible for an individual to launch an effective opposition to the misuse that is being made of our data. Everything else is taken care of by the competent data protection authority, which is not only overwhelmed, but is kept in check by legal and political pressure.

Over and above this particular development, it is also the case that the internet companies in Silicon Valley are now undercutting the rules governing data protection that were enacted in Europe, by transferring our

data to the United States of America. An EU Data Protection Directive of 1995 (which I will refer to in more detail later) fundamentally stated that our data may not be passed from within the EU to third countries that have not put in place any comparable (in other words, adequate) statutory data protection procedures. The USA does not fulfil that criterion, as it possesses neither a comprehensive system of data protection, nor has it implemented any statutory regulations governing data processing activities that take place within the private sector. And yet in response to pressure from economic circles in the US, the European Commission agreed to a procedure in the late 1990s, in which companies from the USA could register on a list that would be drawn up by the US Department of Trade, thereby recognising the principles of what is known as the *Safe Harbour* for data processing, previously negotiated by the European Commission and the US Department of Trade. By signing that declaration, which is monitored by the US Federal Trade Commission, the companies were afforded the same status as a company based in a country that is in possession of adequate data protection regulations. In 2000, the European Commission issued a declaration, stating that the Safe Harbour principles were equivalent to the level of data protection provided within the EU, thereby giving approval for the transfers to the companies based in the USA.

During the years that followed, however, it turned out that for us, as data subjects, it is almost impossible to enforce the principles of the Safe Harbour scheme against companies based in the USA. The primary reason for this lies in the fact that the enforcement in that country is not successful in individual cases, but only in cases involving gross distortions of competition – in other words, in cases involving repeated or multiple infringements of consumer rights. What is more, the majority of people who got in touch with the US Federal Trade Commission were data protection activists from Europe, however individual complaints were rarely admitted, partly as a result of the rules, which are highly unclear. In addition, a considerable number of developments have taken place in the area of surveillance legislation, especially since 11 September 2001, which have severely jeopardised the protection afforded to the data of individual citizens. Those items of legislation particularly include the regulations contained in what is known as the *Patriot Act* and the *Foreign Intelligence Surveillance Act (FISA),* which enables the authorities to access data collected by companies that relate to their customers. Since then, the security authorities in the USA are accessing the personal data, on a major scale, of EU citizens who take up services in the USA, especially from internet companies. Many of these instances in which data are accessed actually take place in accordance with these surveillance laws and the secret jurisdiction that they contain, however the transfer of such data is, in the majority of cases, not in

keeping with data protection law in Europe or with the constitutional principles of the EU Member States. Moreover, and from the perspective of EU law, such instances actually constitute unreasonable incursions into the informational self-determination of individuals. Despite this striking gap in protection that applies to data transfer to the USA, the Safe Harbour statement enables US companies to transfer data relating to their European customers to the USA in an unrestricted way, where it will be accessible to the security authorities of that country.

In October 2015, the European Court of Justice found regarding one of the cases brought forward by Max Schrems to the Dublin Courts on Facebook that the Safe Harbour principles are not respecting the fundamental right on data protection enshrined in the EU's Charter. The judgment follows a request by the European Parliament (in the light of the Snowden revelations on the PRISM program) to suspend the Safe Harbour decision.

If we do not wish our rules governing data protection to be lost in this way, we must take immediate and urgent steps to ensure that the mass transfer of data to third countries, such as the USA, which, in terms of data protection law, are »unsafe«, is only permitted in cases where binding fundamental rules protecting the informational self-determination of all individuals are in place in the country concerned. At the present time, the situation is actually so dramatic, that EU citizens

do not even have any legal entitlement to ensure that the security authorities of the US uphold the protection of their privacy. Under US law, this fundamental right applies only to citizens of the USA and individuals who are permanent residents of the USA. This is a stark example of the way in which our self-determination in the digitised world is being lost at a stroke. If all states afforded protection to their own citizens only, whilst exposing all others to unlimited monitoring and retaining the ability to make use of and disseminate their data in all directions, every single one of us would be supervised on a continuous basis and would be devoid of any rights. And such a situation would certainly occur, once the authorities and companies were to exploit these gaps in protection to the fullest extent, by exchanging data between authorities and companies in the various states. Any regulation aiming to protect our data would then have ceased to apply. In order to avoid this, we must act immediately and fight for a system of effective data protection in Europe and around the world.

The selling off of our data

Every day, we leave countless traces that betray information about ourselves as an individual. Whilst our footprint in the forest can rarely be attributed to us alone, if we pay for an underground ticket using our debit card or read a newspaper online, those acts can be traced back to us using what is known as traffic data. And unlike the footprint on the forest floor, that information will not quickly disappear due to the wind and the weather, but will continue to be stored on hard disk drives, data storage cards or large-scale servers around the world, will get lost in the expanses of the internet and will be read by data-scavenging robots. These collect data like a load of old scrap metal and accumulate it in large stockpiles that enable the programmers that operate the robots to make their profits. Many of these »scrap collectors« – services such as »123people« or »Yasni« – are increasingly in a position to turn these scraps of information into hard cash and sought-after services. Professional data collection agencies, which are sniffing around us like private detectives, are primarily encountered within the information and collection industries. Even before digitalisation got underway, a great deal of information was collected about individuals and their payment obligations and creditworthiness. In the meantime, this has developed into an area of business activity in its own right that is developing with an annual growth potential of up to 20 percent and is increasingly attracting

major investors. As was made clear to me in meetings with their lobbyists for EU data protection reform, increasing numbers of banks, financial services providers and media companies, such as Bertelsmann or Thomsen Reuters, are competing to invest in this emerging sector. Even credit card companies such as MasterCard and VISA have an active interest in the possibility of utilising and selling on our details for a wide range of purposes. At the same time, they regularly attempt to create the impression that the payment details saved by them cannot be attributed to a specific person, but only to a credit card and that this does not, therefore, give rise to any problems in terms of data protection. What the statements made by the credit card companies malevolently fail to point out is the fact that every credit card is linked to a person and a number of avenues are available to identify the owner of the card.

When, in 2013, the credit referencing agency Schufa commenced a joint project with the Hasso-Plattner-Institut in Potsdam, Germany, in order to research the use of freely available information from social networks as part of the process to assess creditworthiness, members of the public began to voice their criticisms for the first time. In fact, this is actually only the tip of the iceberg. Behind closed doors, completely unknown companies, such as Arvato Infoscore, are collecting information about the everyday lives of every one of us and are selling the results of their assessment of our creditworthiness to department stores, mail-or-

der companies and marketing companies. Small-scale providers of micro-credit, such as Kreditech, which is based in Hamburg, even go as far as to collate all information from social networks and carry out a big-data analysis about our lives in their own right, before deciding to grant a loan. Using over 8000 individual items of information (including the amount of time needed to complete the online application), which are linked, for example, to the IP address, the name or the email address of the applicant, the company's own algorithm calculates the applicant's creditworthiness in less than a minute in each case. As a result, the company's turnover during the course of 2013 grew by over 1200 percent. This alone reveals the potential that exists in providing these types of analyses. It is these types of analyses that form the foundation of economic life in the future and represent a new hard currency in the trading of products and services. Our data enable our actions to be predicted and determine the price we are asked to pay. In view of the fact that less than one third of the world's population can be found in the credit referencing databases and the precision of the information held still has room for improvement, there exists an enormous demand for additional data collection and data analysis to take place. Estimating the creditworthiness of consumers is becoming a key service for the future and is one of the largest growth markets of the present age.

It is also true to say, however, that the technology employed and the consequences of the data gathering activities have so far received little analysis in public. From a legal perspective, the majority of these activities are being carried out in a legal grey area. In the commercial domain, hardly any clear rules have been put in place governing the aggregation of mundane items of everyday information in order to draw up comprehensive personal profiles, and governing the use of such profiles as a means of evaluating individuals. The marketing sector is always on the lookout for what it calls *Customer Touchpoints,* at which milestones of consumer activity are recorded and can later be brought together to draw up an overall consumption profile. The number of digital interfaces within our everyday lives is continually on the increase, whether as a result of paying for goods with our debit card or using the online payment system of PayPal, or whether as a result of using a customer loyalty card or receiving a cookie while surfing on the web. All of these touchpoints are capable of gathering countless items of information about the person, his/her purchasing and payment history, interests and life habits, his/her belonging to a target group or the likelihood that he/she will partake of consumer activity. Whether or not we actually consent to these types of data analysis is largely of no consequence any more. Companies make use of legal loopholes or extend their data processing capabilities to an almost infinite degree, without the consent of the people affected. Certainly with the ad-

vent of the multiplicity of apps on our smartphones, if not before, those companies have literally been extracting our data from inside our trouser pockets, and with it, our money.

The first ones to genuinely earn large amounts of money from data were frequently criminals. Even back in the Middle Ages, criminals were able to generate profits by falsifying documents. People fell victim to deception and were duped out of their worldly possessions, due to the fact that bogus information about a trading partner or any official bodies involved appeared to be credible. What, at that time, was limited to only a few points in time during an individual person's life, such as an inheritance, the purchase of land or a doctoral certificate, gradually became an everyday problem. Counterfeit entry tickets, banknotes or passports – with improvements in technology, the copies became ever better and were worth producing, even in the case of crimes that were limited in scale. As a result of digitisation, this problem has taken on an entirely new dimension, however. Whether we are talking about the millions of items of user data extracted from Sony's game console system in 2011, or the hacking into 16 million e-mail inboxes, mainly of users in Germany, in January 2014, it is becoming ever easier to gain access to large quantities of sensitive data about us, a fact that has enabled perpetrators to inflict far-reaching damage in the shortest possible time. Not only is it possible to create new forms of manipulations by means of programming, in order to copy or abuse the *source code* –

in other words, the information – relating to a product or service, it is the local and physical relationship to the item being manipulated that is no longer available, with the result that the persons involved lose a significant degree of control. It is therefore not without reason that in the past few years, we have witnessed a dramatic upsurge in cases of deception involving the use of information technology. Anyone who examines the crime statistics (such as those from Eurojust from 2010 and 2011) will observe a massive rise in these types of crime. A core problem behind this particular trend is what is known as identity theft. Whereas in the past and at present, the most frequent form of identity theft involves credit card numbers, cardholder details and passwords, the identity theft of the future will take the form of an out-and-out race and will involve increasingly obvious security and identification characteristics. Today, laptops and smartphones are, for the first time, being fitted with fingerprint detectors or even iris scanners in order to enable the authorised user to be identified in a manner that simply cannot be falsified. Given this race to incorporate new security characteristics, however, verifying each of these is actually becoming more complex. Due to the fact that a great many interactions no longer take place in the form of a physical meeting between individuals and purely involves interacting with virtual persons or machines, it is no longer possible to make use of information that can only be verified in the flesh. Just as a 15-year-old boy operating from his bedroom in Sweden is able to

utilise the benefits of the internet and take on the identity of a real or invented 32-year-old businessman from Bavaria and conduct business transactions on a massive scale, the organised criminal gangs of today are increasingly capable of managing their activities from letterbox companies in tax havens or via servers located in Ukraine and receive payments via accounts held in Germany. The commercial sector has only taken up the challenge that faces it in the digitised world in a half-hearted way, however. Up to now, each additional security feature that has been introduced has merely led to the invention of additional means of falsification or manipulation being developed within only a short period of time. Unfortunately, human control and individual self-determination have not played any part in the debate, even though they would actually form the solution. In a digitised world, it is necessary to ensure that as many data processing systems as possible are as visible, transparent and traceable as possible. This will increase the ability of individuals to prevent any unintended risks or consequences, by altering their behaviour.

But that is exactly what the major market players of today do not wish to see. They are making sure that the processes of digitisation are increasingly kept as invisible as possible from the point of view of the users. Users should be left unclear as to what actually goes on behind the scenes of an application, product or service, as it is this that enables the operator to earn large

amounts of revenue within a short space of time. The best example of this is smartphone apps which, at first glance, are free of charge and appear harmless. Once installed, however, and once the user has been asked to surrender his or her personal details, which is mostly unnecessary (such as in the flashlight app, which continually requests my current location) or only barely in line with the law (such as the short messaging service WhatsApp, which examines all of the user's contact data and transfers them to its own system). And once the data have been provided, the user is then confronted with what are known as »in-app purchases«, in which each individual part of a service requires a further purchase to be made. These massive breaches of data and consumer protection are packaged up and hidden away. In that regard, many of the market players of today are in the same boat as the criminals themselves. Neither of them have any interest whatsoever in ensuring the users are able to track how the processing of their data is carried out and what consequences will, or could, then ensue. Deception, manipulation, discrimination and opaque deal-making thrive due to the fact that they are not easy to see through. In an age that is characterised by data protection, the opportunities for these types of practices are even greater in number, as the mass of information that one side is able to gather about the other in just a few seconds and is able to use in a manner that does no favours to the subject of the data, is almost infinite. This means that for suppliers of products or the providers of services,

taking a purchaser to the cleaners has been made very simple, without them even noticing it. This is especially critical in the case of financial products and insurance policies, which frequently involve risk evaluations and high amounts of cover. In the case of this particular type of products, the entire life of a customer is scrutinised from top to bottom, before any offers are actually made. It is our data that directly determine the price of a home loan or of a life insurance policy. That is one reason why financial service providers, banks and insurers are heavily involved in data collection, either by third parties such as credit referencing agencies or through activities of their own in the area of data analysis and the evaluation of creditworthiness. Even health data are not immune. For example, it has become public knowledge that the pharmaceutical computing centre VSA in Munich passed details of the illnesses suffered by millions of its customers to other organisations, such as the US-based IMS Health. It in turn processed that information and sold data packages to the pharmaceutical industry. The cost of this was only 1.5 cents per patient – that is all it takes nowadays for the fundamental right to data protection of the persons involved to be simply ignored. The trading of our data is taking place increasingly quickly and encompasses all sectors of the economy. Since 2012, the telecommunications provider Telefónica (known in Germany as O_2) has been planning to merge the location data of its mobile telephone customers into profiles and to sell these on to advertising clients. This

however gave rise to resistance from a number of data protection officers. As it happens, this method of data trading has meanwhile become established – though we are never consulted whenever companies intend to use our details for a purpose other than the one for which they were provided.

The insurance company Allianz recently concluded strategic partnerships with car manufacturers, such as Ford, that will enable it to link the issuing of car insurance policies to an agreement for one's own driving habits to be analysed. By offering what it calls »services aimed at specific target groups«, Allianz hopes to achieve an increase in turnover of 500 million euros, solely by virtue of its partnership with Ford. The primary focus in this context involves providing individualised insurance quotations to young customers who are willing to pay. In addition, premium programmes are also planned that will be linked to the driving habits of the policyholder in question. Once again, it is clear what the deal actually involves: We will receive small-scale benefits if we agree for our everyday lives and ourselves as individuals to be scrutinised and examined. As consumers, we will not be informed of the true value of the data provided nor how they are being utilised from a commercial perspective. If we were aware of that, we would perhaps be less willing to sign up to a deal of that type. Did you know that a long-term study of your acceleration, braking and steering patterns already generates a unique profile? It is as if

you have provided a DNA sample or a fingerprint, accompanied by information as to where you drove and when, how fast you drove (including how often you broke the speed limit), whether you are able to anticipate the actions of other motorists or whether you listen to loud music while driving. In such cases, the new insurance policies contain a stipulation that the volume of the music should be cut by the vehicle manufacturer. This represents yet another step towards a society that is controlled by data analysis.

Since 1 January 2014, the »Sparkasse« (savings bank) in Germany has also offered a direct car insurance product, in which a telematics box acts like a flight data recorder in that it continually records all of the individual information relating to a journey. The data is then passed on to the telecommunications company Telefónica so that a score can be calculated. The value that is calculated in each individual case, which is meant to represent the risk associated with the types of driving displayed or of the individual driver concerned, is then used as one of the factors that determines the insurance premium that is charged. Under the car insurance offered by the Sparkasse, anyone who allegedly drives in an unconventional manner or drives a great deal at night is required to pay extra. As far as the insured themselves are concerned, and taking into account the cost of having the telematics box fitted to the vehicle, taking out an insurance contract that makes use of live data is only worth doing in a small number

of cases. This is not effectively explained to consumers, however, but with every additional customer that consents to this additional type of self-surveillance, it is increasingly likely that those who refuse to allow such a comprehensive analysis of themselves and their driving patterns will be required to pay more. Thanks to the big data used by financial services providers, the doorway to discrimination is wide open.

In this situation, we are witnessing an increasing number of examples, in which the principle of equality and the prohibition of discrimination are completely invalidated by virtue of the day-to-day practices involved in the mass collection of data. At the end of the day, the facts that can be calculated using the mountains of data collected cannot lie. The fact that the meaning of these »facts« for the purpose of reaching the decision in hand is very much in the eye of the beholder and that in the majority of cases, the decision-making criteria form a service provider's best-kept secret, is illustrated in the case of the International Air Transport Association (IATA). Within the IATA, all of the major airlines agree upon common standards and regulations in the form of a self-regulation scheme. Since summer 2013, it has been known that the IATA bodies are negotiating about the personalisation of ticket offers by all of the member airlines of the organisation. The plan is that anyone searching for an airline ticket will be required to register first of all and that the identity of the person carrying out the search will be determined

using the information already available. In view of the fact that the airlines have already been collecting personal data in large-scale reservation systems for decades and sharing these with travel agencies, hotels, car hire companies and criminal prosecution authorities, they will already have access to a considerable quantity of information that they can use in order to draw up a highly-personalised profile about almost anyone. The result of such an agreement between airlines, which would somewhat resemble a cartel, would be that any enquiry about available flights would be preceded by an extensive analysis of the person carrying out the search. It would be fairly certain that anyone who is quite clearly limited to specific flights, perhaps because he or she always flies on a specific route at the same time, would be shown a different price for the same ticket than a flexible tourist on the lookout for a bargain. There is also a possibility that they may only be offered different flights, as popular routes will only be offered to clients with deeper pockets, whilst the managers are not willing to book a more favourably-priced package flight. That decision will be taken out of the hands of the person carrying out the search. They will be categorised on the basis of information held by third parties and, as a result, will ultimately be taken to the cleaners, as the algorithm on which the decision is based will be owned by the airline. As customers, we, on the other hand, will become completely transparent and will be easy prey for rip-off merchants and cartels such as the IATA.

It is certainly nothing new that monopolists and cartels enjoy considerable scope to apply discrimination and are able to push through unfair deals. This phenomenon also existed in the past, which is the reason why competition law and consumer protection law came into being. As a result of the power that is exerted over our data, however, it is becoming increasingly difficult to enforce those rules. If we have no power to make decisions about how our data is to be used, we will be unable to trace the effects of any discrimination that occurs. That is why many companies and their lobbyists are attempting to reduce data protection to the current aspects of competition law and consumer protection law and to eliminate the aspect relating to fundamental rights from the relationship that exists between us, as data subjects, and the private-sector data processing companies. By doing so, they are also manifesting their disproportionately strong position in relation to the consumers, due to the fact that they enjoy the exclusive right to determine how the data are actually processed. The only situation that will restrict their activities will be if this approach results in a massive distortion of competition or if a situation arises that is regarded by the majority of consumers as unfair. Generally speaking, however, it will not come to that, due to the fact that we, as individuals, do not possess the evidence, the time or the financial resources to associate our own case with that of others and to win a court case relating to consumer protection or competition law. Only once in a blue moon will strong

co-petitioners or large-case consumer protection organisations have the opportunity and the resources to see a legal case of that type through to the end. In the majority of cases and after years of tough argument and debate, the few sets of legal proceedings that take place end in a compromise that is favourable to the companies. Alternatively, the proceedings are terminated, with the result that there is no real change in the approach adopted by the companies concerned. As a fundamental right, such as in Europe for example, data protection provides the foundation that ensures individual legal protection for an individual process applied to data. If the rules have been configured to include an effective implementation mechanism and if independent data protection authorities are available to be contacted and are furnished with an appropriate level of resources. Unfortunately, this is something that is still under development. And even in Germany, which over a number of years has achieved a relatively high level of data protection, the application of that mechanism is continually being suppressed by economic and political factors.

Clear rules to govern the digital market are needed, and they have yet to be successfully established. Time and again, regulatory approaches have been adopted which have missed the mark, for example with regard to copyright, where better law enforcement has been pursued only by means of more comprehensive protection of copyright works. The only useful instrument to

regulate the market was EU competition law, which, thanks to action taken in individual cases by the guardians of competition, was able to bring about better enforcement of fundamental rules. But in an everyday life dominated by the digital world, that will not be enough. The European Commission ought now finally to submit proposals for legislation on a single digital internal market for the European Union. This would be analogous to the way in which the Commission set in motion a reform of data protection law with the entry into force of the Lisbon Treaty and the EU Charter of Fundamental Rights. The Commission proposal of 2012 and agreement on a position in the European Parliament in 2013 on an EU General Data Protection Regulation represented two major steps towards effective rules for the digital market, to which I shall return in detail later. But elsewhere, the European Commission and the governments of the Member States delayed important initiatives on net neutrality (equal treatment of internet users and content), exploitation rights (rights of copyright holders, acquirers and users of intellectual property) and freedom of information (publicity of information, particularly about societal processes, institutions and undertakings). In connection with data protection too, the German Government played for time for a good while because the Ministry of the Interior was protecting the interests of large IT businesses which, at internet summits, repeatedly told the Ministry what an adverse economic impact the adoption of data protection rules would have on them.

This is another subject to which I shall return. It plays into the hands of all those who do not want democratically determined rules in the digital market.

While big businesses such as Google, Amazon and Facebook extend their market power to ever new sectors of the economy and even create their own – self-regulated – digital markets, the European Commission and governments seem to be groping around in the dark. At present, other than data protection reform, there are no serious proposals for regulation of the digital internal market. The long awaited proposal from the European Commission for a regulation on the telecommunications market, which would unify the rules on internet services, turned out to be a pure lobbying paper, containing no genuine restrictions with the aim of protecting consumers and smaller market players. The rules that the European Parliament wished to see adopted concerning net neutrality were not included even in rudimentary form. So far, the IT industry lobby, particularly acting on behalf of operators based in the USA, has succeeded in opposing any genuine regulation in Brussels. They are investing millions in lobbying against legislative proposals such as the General Data Protection Regulation, because they know very well that their billions' worth of profits are made by breaking the very rules which competitors and consumers would at the very minimum expect in a digital market. Internet giants based in Silicon Valley are in the vanguard of efforts to disseminate an ideology

which basically has the aim of defeating any State regulation. They regard data protection as the final hurdle that they need to overcome in order to capitalise on the areas of life which up to now have remained the most private and intimate, and to subject them to their market logic, to the detriment of our informational self-determination and privacy. This means that all of our data are being put up for sale, and we shall only be able to stop this if we are able to regain sovereignty over our own data.

How can we achieve data sovereignty?

The existence of the World Wide Web means that, at first sight, any attempt to introduce binding data processing rules is predisposed to fail. Anyone attempting to do so must be aware that any rule can be bypassed simply through manipulation of the data processes. This could occur, for example, simply because the processes in question lie outside the scope of their own rules. In contrast to the situation in the analogue world, where goods and services first have to cross physical borders, it is virtually impossible to impose border controls in the digital world. Such controls would also destroy much of what liberal democracies have created: privacy of communication, freedom of information and opinion, open borders and markets, and even data protection itself. For, logically, controlling the flow of data presupposes control of the data themselves. Most countries have already reached this conclusion. Within the ITU (International Telecommunication Union), many countries are considering the introduction of *Deep Packet Inspection.* This would involve in-depth monitoring of virtually all data packets and reading their content. It would lead directly to the monitoring of all communications, a practice that is manifestly already adopted by secret services around the world.

As constitutional democracies, we should clearly not follow this trend. What is more, the fact that it is precisely the world's non-democratic, repressive regimes that favour such action should act as a wake-up call. Nor is it appropriate for the increasing calls for regulation to make reference only to the United Nations or to »international rules«. For despite what the Western democracies seek to suggest, it is no longer a foregone conclusion that agreement can be reached with the rest of the world on the effective protection of fundamental rights. Liberal constitutional democracies have also acted in breach of their own values and rules for far too long. Only too often have exceptions to fundamental principles been established in the interests of what are deemed to be more important goals. Given the NSA affair and the vast scope of the surveillance undertaken by the secret services, it would no longer appear realistic to speak of joint transatlantic rules that meet the standards of the human rights conventions.

Despite this, it is obvious that a solution to the problem of loss of digital self-determination can only be achieved through a cross-border regulatory framework. What we need, therefore, is the conscious establishment and implementation of legislation by all those countries that are seeking to effectively safeguard the human right to data protection. Meanwhile, our data traverse entire continents in a matter of milliseconds. When someone sends an email from Vienna to Munich, it frequently passes through North America or India before it reaches

its addressee. If we examine the wide range of rules that should apply to cross-border data processing, it is clear that there have been many legal approaches to the problem since the Nineties, but that these frequently highly academic alternatives have still not brought legal certainty. As a result, even where the processes involved are very simple, our data may pass through several legal systems without our knowledge, simply due to the location of cables, servers and headquarters. Traditionally, each of these legislations applies the rules it has introduced itself. This ultimately generates a problem that is threatening democracy itself: should my judicial area allow other legal systems (which I have never legitimised directly or through parliament) to be valid within its territory? If so, this would ultimately cause the downfall of a constitutional democracy. It would therefore be both logical and necessary for the European data protection and criminal authorities, for example, to equally pursue players outside Europe or even government bodies such as the NSA through legal channels, if there is no legal basis for their surveillance activities here in Europe. If it should prove impossible to find common overriding rules, then there would only be one alternative: an attempt to ensure that their own law is applied and to penalise breaches, through the application of stricter controls, harsher sanctions or even territorial restrictions on data processing. Failure to do so would cause domestic players to question why they should adhere to the joint rules, while external players actually enjoy privileged status in the digital world.

The initial reactions to the consequences of digitalisation as regards this legal uncertainty were thus targeted primarily at more rigorous enforcement and compartmentalisation. Whereas in the West, emphasis was placed on a cautioning and blocking system, repressive regimes started to impose extensive censorship measures and to close down parts of the Internet entirely. Many laws have been introduced in the USA and the EU since the turn of the century, aimed at better enforcement of intellectual property rights, with the aim of confronting the virtually unlimited opportunities to move online content beyond the borders of individual judicial areas and into legal and data processing systems that are, de facto, difficult to control. Whilst politicians took very seriously the interests of large companies seeking to ensure the enforcement of their legal positions, and pursued this through enforcement measures, some of which were disproportionate, the interests of smaller competitors or even individual players in both the commercial and public spheres fell by the wayside. It also quickly became clear that this action was not only opposed by some groups within society (initially the Web scene, followed by broad circles within the world of jurisprudence and left-leaning liberal politicians), but was also unrewarding. In fact breaches of the law, involving both copyright and personal rights and also criminal acts, extended further into areas that are difficult to control. Both failure to prosecute and the rampant corruption in some countries, coupled with the technical opportunities to evade

most state-of-the-art law enforcement as far as possible (for example by successfully deleting all traces, whereas the police and the justice system had not even come close to tackling the topic of IT forensics in the digital field), were therefore fundamentally responsible for a rise in breaches of the law, in particular by those involved in organised crime. Examples of infringements of copyright include Megaload and Kino.to, while credit card fraudsters and professional data thieves were able to bring about huge economic losses. They had and still have the means and IT knowledge to stay one step ahead of the surveillance by the state prosecution authorities at all times.

Meanwhile, even repressive regimes such as China and Russia have had the same experience; they were fundamentally successful in their attempt to eliminate traditional Internet products (in particular those from Silicon Valley) from their countries by using alternative products they had developed themselves. These products enabled the governments to establish a comprehensive censorship and surveillance infrastructure, which enables them to prevent their citizens accessing virtually all undesirable information, while at the same time gathering at least equally comprehensive information about those same citizens. This enables them to restrict the size of movements that are critical to the government and to identify and detain those involved. The companies affected find themselves in a pact with the Devil; for, like the search engine operator Baidu,

the uncontested market leader in China since Google's withdrawal, they put a gloss on everything. This makes it all the more obvious that Baidu and its 140 000 developers are nothing but the stooges of a surveillance and repressive system that rides roughshod over data protection and fundamental rights. However, it is also evident in China that even a system such as this does not function flawlessly. Using tools such as the anonymisation service TOR or so-called proxy servers, increasingly more Chinese citizens are learning to access microblogging services such as Twitter and to circumvent the regime's censorship and surveillance measures. Other countries have since discovered that although it is possible to tighten up repression and surveillance, this seldom results in better assertion of its own laws or politics in the digital era. As a result of the scandal surrounding NSA surveillance, even the large Internet companies in the USA and Europe are being forced to fundamentally reconsider their own role when it comes to human surveillance. For in this case too, it is not the agents of the NSA or other secret services who gather most of the data from our communications, but the data loggers, the ISPs and the IT companies. I will examine this question in greater depth in a later chapter.

Therefore, if we as citizens wish to regain sovereignty over our data in a networked world, our ability to do so will be influenced by two developments in particular, both of which will have a sustained effect on the balance of power in the globalised and digitalised society: the development of technical alternatives

to the current world that relies on mass, uncontrolled data processing, and the creation of economic alternatives through the establishment of a legal and political framework. These two developments are interdependent. Only technical emancipation from the IT giants and their monopolistic activity, through the involvement of humans in the design and use of technology, equipping them to use it responsibly and mindfully, will generate political and legal change that is supported by most of society, and which will ensure that the foundations and principles of an enlightened and democratic society are carried forward into the digital era. What is more, such technical emancipation will never be achieved without political and legal initiatives that are designed to strengthen a countermovement to modern data gathering and surveillance structures. Competitive alternatives to the practices employed by today's Internet giants can only be achieved if important markets make an economic choice on the direction to take.

Therefore, to create the prerequisites for human emancipation in the digital era, we need to see what amounts to something akin to a revolutionary impetus, in which political pressure by the public compels the political decision-makers to effect such a radical change of direction. Whereas between 2001 and 2013, only very few people viewed this as realistic, with the vast majority being far from willing to recognise the importance and necessity for such change, the disclosures of Edward

Snowden triggered a social process of acknowledgement, which can trigger such a revolutionary change in the way personal data was previously handled. It would appear that the risks to the lives of individuals, and consequently the importance of the topic to politicians, have not yet been fully acknowledged. However, young people who are already familiar with digitalisation are drawing initial consequences, and Internet giants such as Facebook, Microsoft and Google are seeing this reflected in falling user numbers.

In his Christmas Message broadcast on British television, the whistleblower Snowden went straight to the crux of the matter: A child born today will grow up with no conception of privacy at all. They'll never know what it means to have a private moment to themselves, an unrecorded, unanalysed thought. And that is a problem because privacy matters. Privacy is what allows us to determine who we are, and who we want to be.

Despite the far-sighted and courageous action of both Edward Snowden and of activists and journalists, who have conveyed their findings to us, the political challenge could become even greater. We are not only facing the greatest opponent imaginable in this dispute with the secret services of all countries and the largest companies in the world. In fact, and above all, the lack of technical knowledge in broad swathes of society, and consequently also in politics, the media and the legal system, is pre-

venting a process of re-regulation of data processing and recovery of the strength of data protection. This is all the more important because all these sectors of society stand to gain extensively from the exploitation of all our lives. The re-election of President Obama in the United States for a second term came about largely as a result of the comprehensive and calculated analysis of the potential electorate. Even now, for many politicians and parties, and also for many initiatives within civil society, this is seen as a positive example of how to encourage electors to vote en masse. At the same time, the entire media sector is experiencing its most radical change ever, in which traditional entertainment media and also newspaper and book publishers are fighting for their lives, and all those media companies that are not acting in the spirit of the times and hand-in-hand with the business model of online direct marketing based on Big Data, in which the personal data of readers or viewers is analysed on a massive scale, to enable them to sell bespoke advertising and attract a larger public to their own products, appear to be going bankrupt. Data pooling has become the lifeblood of the entire media industry, which had been failing for years to open up new sales channels on its own initiative. Last but not least lawyers, few of whom specialise in new media and IT law, have been signed up by large IT companies in particular and are not to be found in universities or in the world of politics; as a result, jurisprudence in this field has allied itself with the interests of large groups and the data processing industry, which is a cause for concern.

The importance of examining the consequences of digitalisation on an independent basis was seriously underestimated for many years. The Internet giant Google has now taken on this role, and finances research institutes and NGOs around the world. Politicians were too slow to react to these developments. The former coalition between the CDU/CSU and the FDP set up a Data Protection Foundation, which was so under-resourced in financial, human resources and conceptual terms that it gave the impression of having been set up in order to put the topic on the back burner for a few years. Added to which, by appointing the CDU politician Andrea Voßhoff as the new Government Data Protection Officer, the Grand Coalition filled a key post at the data watchdog body with a politician with little or no prior experience of the work of data protection officers or of previous debates in the field of data protection policy and law. In doing so, it has weakened the office of the independent Data Protection Officer at a time (immediately after the NSA affair had come to light and when EU data protection law was in the throes of being restructured) when the challenge associated with the political and societal transformation to the digital society is extremely high. We can only hope that Voßhoff will demonstrate her independence from the Government, and will defend data protection as a fundamental right, on behalf of all citizens, against attacks by the state and businesses.

The neglectful handling of data protection by large sections of the political world, and the challenges of digitalisation, are also evident from the fact that reservations concerning the virtually indiscriminate opening up of the digital market were ignored for years. There followed a spiralling decline in citizens' and consumers' rights in the digital world, which has become unstoppable. We will only regain sovereignty over our data if this decline, irrespective of its speed, is halted. Unfortunately the political world is still turning this wheel because, driven by trade associations, investors, rating agencies and banks, it wants to exploit the growth of the digital market in the interests of the economy. In the view of the trade associations, the question of data protection regulation is reflected in actual employment figures. They believe that every upheld or even additional rule imposed on the digital market threatens the welfare of entire economies. As a result, politicians on both sides of the Atlantic continue to run after the major IT groups, who promise something akin to utopia. In times of economic and budgetary consolidation, this represents nothing more than a virtually unaffordable glimmer of hope for politicians.

What is more, consumers have repeatedly made it clear to politicians over the past few years just how little they appear to care about the protection of their most intimate data. At least, we have given them cause to assert this. We have done so by constantly acquiring new smart phones and Internet applications, which analyse our day-to-day life and our personality, and by irrespon-

sibly disclosing our personal information and wafting it out into the ether without fear of possible consequences. This must have given the impression that we, as humans, no longer care about the sovereignty of our own private space and our personal data. The Minister of the Interior and the lobbyists for the data loggers immediately exploited the initial suspicion about this development by ringing in the end of data protection. They maintained that as humans, we forfeited our human right to data protection by flinging our data around indiscriminately. »Young people« in particular, who disclose everything about themselves online, could not claim protection from any of the consequences of their youthful exhibitionism. This argument, the disclosure of which was disastrous for politicians, was common sense for years, and frequently used to divert attention from the failure to effectively enforce privacy laws. Given the constant stream of new surveillance and data scandals, some of them advised us to communicate less online if we feared potential violations of our private space. The underlying message hurled defiantly at people was nothing less than »deal with it yourselves«. It is as if politicians had responded to people's reservations about possible traffic accidents following the development of the car by saying: »If you're worried about being run over by cars, just don't go on the road.« Most of the key politicians responsible have never even given a thought to the fact that it is a matter of laying down and implementing the rules of the road in the digital age. So, if we want to regain sovereignty over our data, we need to change this.

To change our politicians (or rather »us«, as I am not seeking to exclude myself from this group), we also need to change ourselves to some degree. With the advent of Big Data and ever more data analysis applications, consumers have also played a significant part in the way our society has developed. The drive towards ever more technical options and ever more advanced networking of our world inevitably leads to an increasingly entrenched surveillance logic, if there is no categorical shift away from the inherently associated processing of personal data. Whilst video surveillance of one's own garage or garden was just the start, the private drone or live location of family members and supposed friends via GPS will undoubtedly not be the end. An indiscriminate involvement in any technical innovation claiming to improve our lives guarantees that we won't become aware of the huge consequences until it is too late. The best example of this is seen in the newly developed miniature cameras, which operate using the Internet and face recognition software. As early as the 2010 CeBIT IT Fair a video was shown at the launch, in which a young woman holding a smart phone is going up an escalator holding the camera towards a good-looking young man coming in the opposite direction. His face is immediately recognised using his biometric features, and compared with the photos of him available online. Every hit brings up further information about him, for example on social networks, on his employer's website, his wish list at an online shop or in the discussion forum of a self-help website.

Without exchanging a single word with the person opposite us, and without that person being aware, we suddenly know everything about his life. As a result, statistical information is not scrutinised and human contact becomes ever rarer. The development of the Google Glass data eyewear takes this detachment from the former social reality to a new level. All of a sudden, any situation, however intimate, can be recorded by the integrated mini-camera and posted online. In developing Google Glass, Google has taken a further step towards the full-blown digitalisation and recording of our day-to-day lives. Now that Google Streetview and Google Earth have surveyed and made visible the entire world, and the first driverless cars can already be seen on the streets of San Francisco, even the pedestrian has now become an analyst, constantly filming or photographing the world's objects and people on behalf of us all, tagging them and linking them with information using face or building recognition software. Google applies the following rationale: Once data eyewear has become established, there is nothing to stop the campaign of de-anonymisation of the entire world. For everyone will make an active contribution towards ensuring that even the very last unbeliever or reluctant participant will be drawn into the fully recorded and monitored data world. No-one will any longer be able to back out, or ultimately prevent us constantly recording information and making it retrievable or accessible somewhere. The best example of this is face recognition, which Facebook has used on the photos posted

on its network. The facial features of every image posted are scanned and immediately compared with all the other available images on the network (or on the entire Internet). In this way, a person who has made an explicit decision not to publish data about themselves and their life on Facebook will quickly become visible, and will be tagged and linked to information by the members of the Facebook network. The company does not offer effective ways for that person, as an outsider, to find out what has happened and to remove the data in question. We will no longer be secure even at our most intimate moments. The possibility that on your next date, someone wearing Google eyewear could film the progress of your lovemaking is no longer only conceivable in the realms of science fiction. Data gathering is becoming increasingly less predictable or obvious to the person who is targeted. The whole thing could even be transmitted on Livestream, without you even being aware.

The acquisition of the thermostat and smoke alarm manufacturer Nest Lap for a mere 3.2 billion US dollars indicates that Google is already seeking to penetrate these most intimate areas of our lives. These are smart metering devices, with which our home (and also Google and all those who profit from our data) knows at any given time when and where we are within it and what our habits are. Guests are of course also registered, along with the way in which we use certain equipment. And there is more: games consoles and

smart TVs linked to the Internet record which games or television programmes you like, how long you play or watch them and through which channels you zap. Everything is personalised, via the user account that you initially set up. Or your electricity provider offers you a better tariff if you agree to fit a smart meter, data from which measures power consumption in milliseconds, with the aim of improving energy management. In most cases this impacts on your privacy, because anyone living alone will quickly provide a precise profile of how long he is at home and what his cooking or viewing habits are. The same applies to the smart refrigerator or any other conceivable device linked to the Internet, all of which generate and distribute data about your life – at least until such time as consumers decide against this comprehensive surveillance. Many of these services would be equally achievable without the need for personal information to be continuously passed on externally. It would also be possible to simply present a range of profiles for selection, which could be developed in such a way that only a broad description of one's personality would need to be revealed. It is up to us to demand such alternatives! Otherwise, data gathering by all of us will know no bounds. There is no doubt that this constitutes an ethical debate on the boundaries of what is socially acceptable. As an example, how do we handle this example from Barcelona, where a bar decided to set up a speedier payment option by asking customers to have a data chip carrying their credit card information implanted under the skin

of their thumb? Or do we wish to allow mini-drones, which can easily be mistaken for a bee, to penetrate and film everywhere, freely and undetected? What are the limits to the digitalisation and networking of our lives, humanity and our environment?

The personal surveillance that we ourselves instigate, or at least approve, is starting to appear reckless. The acceptance of the advancing loss of sovereignty appears almost totalitarian, if we consider the consequences of the sacrifice of self-determination on society as a whole and on any minorities. Whereas when digitalisation was in its infancy, perceived discounts in particular, albeit very small, encouraged us to disclose our own lives and personalities as widely as possible, through the use of loyalty cards and competitions, nowadays there are numerous data loggers that we set up ourselves, and which illuminate every corner of our daily lives: examples are the calorie counter, which records in detail what you have eaten and drunk and when, the quit smoking app, which records your own smoking habits, the sport app, which records precisely how many metres you have jogged and in many cases, even publishes it afterwards. We create a digitalised image of who we are, which uses sophisticated development tools to generate a far more accurate picture than could any doctor or psychologist following a thorough assessment. At least, when it comes simply to making a calculation based on as many data as possible.

The Big Data about you yourself is bound to generate an optimisation logic. For once the fundamental data are available, the initial areas needing improvement become evident. Live more healthily, work more efficiently, cook better, find a partner more quickly – Big Data finally reveals the virtually limitless opportunities and potential for physical and personal self-improvement. When we use all these new apps, we also create the basis on which all these programs function: Big Data applications can only deliver meaningful added value once they have a huge volume of comparative data from other users and from all the personal profile calculations. Free alternatives to the full products are often available; these act as data providers, in return for which they offer very limited use without charge. In any event, a free or cheap offer is only an option because personal data are released in return. The provider takes what it can get. If users give their contact details, calendars and location data, because they do not question the need to provide them, these data also continue to be used for analysis and other purposes. As adult and self-determining consumers, it is undoubtedly our duty to question why we repeatedly allow ourselves to be stitched up in this way and to voluntarily provide so much data without getting what we really wanted. As an example, we should ask ourselves more often whether the practical results of the Big Data analysis are in fact so important to us that we are prepared to make ourselves more transparent to the operators or third parties who gain access to the data than we would

to a confidant or to our doctor. Must we first record, measure and calculate everything in our lives, in our relationships or in our bodies in order to acquire information that is meaningful to us, or is such an analysis perhaps nothing more than an exciting way of keeping ourselves busy, which does not merely discourage us from self-determining action based on an intellectual examination, but also obviates the need for such an examination. An inspection of the Big Data analyses will quickly show that they are rarely the solution to a problem, but can merely provide stimuli. Anyone seeking such stimuli does not really need personalised analyses; they may safely rely on anonymous statistics.

If nothing else, would it not make sense to ignore or even oppose the Big Data efficiency enhancement logic simply because it makes us into machines being driven to the limits of their efficiency. For that logic will make society into a sterile place full of clean clones, who act according to the rules of efficiency and logic rather than in the pursuit of meaning, happiness and humanity. The path towards the recovery of sovereignty over our data also involves recovering our self-determination and taking responsibility for our own lives in the digital era. There is a greater urgency than ever before for us to take this path. The mass analysis of our personal data makes the neoliberal logic of the exploitation of human life into the all-encompassing mantra of the post-modern world. The image of Big Brother controlling everyone is no longer an evil ruler,

but a society that controls itself, and which is made omnipresent and inescapable by the technical tools for self-optimisation that are available. If we want to stop this development, we need to recover self-determination when it comes to our data. Only then will we be able to make a decision on the extent of our personal and collective self-disclosure in full knowledge of all the circumstances and consequences. Without doubt, every individual will have to make the final decision on the release of their own data. The law and the social environment can only empower us to act. By implication, we also have sovereignty over our own data and our own person, and can decide ourselves whether to release information. However, here too we must be in a position to make our own decision in a state of full awareness. In order to achieve this, we must deal with all the pressures and circumstances to which we are exposed on a daily basis when our data is gathered and processed.

So we should question whether we do in fact wish to be subjected to the market logic design that seeks to compel us to become involved in calculable consumption. Would we not rather make our own decision on which product and what degree of self-disclosure are right for us? In order to gain our own and society's sovereignty over these circumstances, and to create a situation in which the rules can be debated openly and established responsibly, we need, first and foremost, transparency and ways in which to intervene. This is where data pro-

tection principles come into play. They are designed to set out the situation for us and to react to it accordingly. Only in this way can we decide ourselves whether to insist on our right to declare something to be a private matter, or are prepared to disclose information about ourselves either individually or collectively. The highly complex Big Data applications and automated data processing, which have become utterly impenetrable without special technical knowledge, make this principle all the more important. Nowadays, the algorithms such as the search engine Google, and the decision-making logic behind profiling, scoring or data mining, are impenetrable to most people. It would therefore be absolutely necessary for the processes to be made visible and comprehensible, and for them to be examined for potential breaches of the law or undesirable consequences. This is the precise aim of the idea mentioned above, which has been put forward by the algorithm designers, who are of increasing relevance to society. The need for companies and authorities to disclose the logic or even the actual procedure behind the automatic processing of personal data has long been the subject of debate, under the catchphrase »Show me your Algorithm«. The example of the credit information agency Schufa, whose mass data gathering regarding our creditworthiness was recently the subject of a ruling by the German Federal Court of Justice, which found that Schufa is not yet obliged to disclose the algorithms used in its calculations, demonstrates just how important this is. This could change as a result of

the EU Data Protection Regulation. The most recent EU financial market rules are an example of how this could function. In these rules, the European Parliament has ordered that the algorithms for the computerised trading in financial products must be approved before the financial market players will be permitted to work with them. The intention is to prevent harmful speculation and clever circumvention of certain rules or even of entire legal systems. This step would also be a further aspect of important sovereignty rules in the digital era in the context of the consequences of the processing of personal data.

In the pursuit of a self-determining digital society, in which data protection is a fundamental principle of coexistence, everyone must go through a learning and emancipation process, both personally and in relation to politics, the media and the law. The next few years will be critical in this regard. As Europeans, strong data protection in the European Union, implemented consistently throughout the EU, will be critical for us. Only in this way will we have the opportunity to tackle with confidence the cross-border challenges of the globalised and digitalised era. A broad supranational debate on the core values of our coexistence in a global society is emerging. In the long term, we require nothing less if we wish to enshrine these core values permanently. Nonetheless, to achieve this will require considerable staying power, coupled with some important intermediate stages, which are bound to give rise

to difficult confrontations between self-determining citizens on the one hand and the data-hungry and power-mad players on the other. It will take a self-aware, networked society, which will make the effort to carry forward the balance between reciprocal control and self-determination, between rules and autonomy, which has evolved and been fought for over the centuries, into an era in which the means and opportunities for repression have expanded just as swiftly as those for emancipation. In this context data protection, hand in hand with freedom of information, represents the primary driving force of an emancipated and networked society.

The networked society

Whereas the challenges for data protection and human self-determination highlight in particular the risks associated with globalisation and digitalisation, there is no doubt that networking humanity has brought us all a step closer together. Instead of isolated national states and market barriers, the removal of borders, the opening up of markets and the establishment of the World Wide Web have led to a global information society. It has become easier to escape from the structures of familiar systems, to find supporters for our own ideas and views and to develop new creative scope. The arrival of communication via the Internet has suddenly brought together widely dispersed individuals, who are able to create something together. Digital networking has opened up far more opportunities for structurally weaker players, oppositionists and minorities. Despite all the uncertainties about the long-term effects of technologisation and digitalisation in every area of life, there is no doubt that the Web has brought a new dimension to many individuals and movements. Of itself, a media-dominated era makes it easier for many players to get their messages out into the world and find supporters. In the social networking world, the number of supporters quite simply carries more weight than structural power. The Web »natives« and their digital progeny in particular have experienced how democracy can also function in globalised and digitalised eras.

The most famous example is undoubtedly the Arab Spring, which brought unrest and revolution in countries of the Arab world such as Libya, Egypt and Tunisia in the Spring of 2011. The new opportunities for networking between individual activists led to the establishment of a counterpublic, which was ultimately able to bring down the existing regime. The role of infrastructure control also became highly evident. When the protests began in Egypt, former President Mubarak exerted powerful influence over the infrastructure of the Web, and in some cases reduced Internet access to an absolute minimum. It was also possible to track the online activities of dissidents. As a result, the role of data protection was critical in terms of the opportunities available to such individuals. Control of online systems remains an important tool employed by repressive regimes. In Syria, Bahrain, Iran and China for example, controlling use of the Internet and blocking certain content, or even all Internet traffic, is an everyday occurrence rather than a rarity.

Many people around the world are fighting to prevent this. Under the US Government plans for the Internet statutes SOPA *(Stop Online Piracy Act)* and PIPA *(Protect IP Act)* , both projects designed to improve the enforcement of intellectual property online, thousands of US citizens protested against the restriction and control of their online activities, thereby preventing a good many of the proposals, which were designed, for example, to block Internet access by alleged criminals

or to close down suspicious websites. There was similar conflict in Europe: By exploiting the new scope for influence offered by the digital era, citizens throughout the EU campaigned against the ACTA *(Anti-Counterfeiting Trade Agreement).* This was a multilaterally negotiated draft Agreement designed to permit improved enforcement of intellectual property on the Internet. As a result of their efforts, the Agreement was rejected by the European Parliament in June 2012.

Legislation such as SOPA and PIPA, and also the ACTA Agreement, would in particular have meant invasions into the data protection of Internet users, i.e. of almost all citizens. For an analysis of all online communications would have been necessary in order to establish a breach of the law through stricter and automated enforcement. However, the drafts of the legislation never envisaged protective provisions designed to prevent disproportionate unauthorised disclosure or sustained legal protection. The fact that they experienced little opposition during the years of preliminary negotiations among politicians and in society is therefore all the more surprising. It is still not sufficiently clear, even to those responsible, what consequences such ostensibly technical legislation would have on our society and on people's everyday lives. It required the critical brains of young activists who have grown up with the Internet (from, for example, the civil associations »La quadrature du net«, »Digitale Gesellschaft«, »Panoptykon Foundation« and »European Digital Rights Initiative«) to provide initial, all the more important thought-provoking momentum.

Not only did this involve taking a clear stand against the ever-advancing legislation on international trade agreements; the European Parliament also won an important role for itself as the representative of citizens' rights in the digital era. The conflict surrounding ACTA withdrew the niche status of the Net movement and, not least, made many people aware how important it is to protect fundamental rights at a higher level.

ACTA was rejected against the background of several months of protests in Europe and around the world against the restriction of freedom of information and data protection through imprecisely defined but severe law enforcement measures. It demonstrated to many people that it is also possible to fight successfully for one's fundamental rights both in the digital arena and internationally. Networking helped to ensure that the campaign for personal rights on the Web was successful. Many people, in particular the young, who exchange data on social networks such as YouTube, Facebook and Twitter, were politically interested and motivated during this conflict.

For a few years, the networked society was made up of an elite group of people who felt at home in the digital world. There was already some successful campaigning for the preservation of citizens' rights in the digital era. However, in the case of the software patents, the EU telecoms package of directives and regulations, censorship of the Internet and the agreement on the transfer of SWIFT banking data to the USA for example, these

successes simply involved preventing misguided attempts by a political world that was not focused on the digital environment. Success in relation to the ACTA is the starting point for society to tackle the question of »How else?« in relation to regulation of the Net. This is a conflict that has now moved to centre stage in the political debate, albeit ten years after the first »Not like that!« battles.

However, the question now being asked brings responsibility. The digital revolution demands answers from those who are still figuring out the digitalisation processes. They need to explain where the digital world interfaces with the values and rules of the analogue world. It is they who carry responsibility for defining properly functioning rules.

The rejection of ACTA was unquestionably a decision of far-reaching significance, not only for European democracy and the rights of Internet users, but primarily for those who want future-proofed and enforceable law in the digitalised and globalised era. It represents the perfect opportunity to re-regulate the rightful interests of all those involved, in the form of a digital social contract. The charged-up debate surrounding the ACTA Agreement made the conflict surrounding the wrong decisions made in the past abundantly clear, highlighting the gulf between two parties at loggerheads, generally referred to as »the users« and »the holders of rights«. However, the fact that ACTA was ultimately rejected means that both groups were winners. For the Agreement would have widened the gulf between them

without solving a single problem. Instead, how the works of copyright holders in the digitalised era can be protected, and how their royalty claims can be enforced in accordance with both national principles and the fundamental rights of the other parties involved, can be clarified in an open debate. Politicians will also have to be involved, using the debate on data protection as a model. The complaints by editors, publishers and authors about the serious financial situation of the sector are unquestionably alarming, because the very essence of our free democracy would be under threat without them. The degree of social involvement in culture and the media has always been an important indicator of human freedom. As things stand, we have always managed to survive periods during which cultural and intellectual variety is restricted. Whereas in the past, this was driven either by repressive cultural policy and by the absence of any cultural policy, nowadays it is powerful profit-hungry corporates who are seeking to force our cultural and informational lives to conform with their model. Having been an arena for creative design and open networking, the Internet is now moving in an entirely different direction: governments, monopolies and criminals are assimilating the structures of the Net, making them into nothing more than a powerful means of gaining control – not over markets, but over people.

It is not only creative people who are falling by the wayside. It is evident that as regards data protection law for example, decisions previously taken by society have long since been called into question. If we use one of the many Apple devices, have a Facebook account or allow ourselves to be identifiable to Google – we are all becoming increasingly aware how little these companies care about our rights and aspirations. And they can afford not to care. There was a time when their founders supported the idea of co-existence in solidarity within a revolutionised virtual world, in which everyone would be able to participate. Now it's all a question of who has more users, exchanges more content, has higher advertising sales, or quite simply has the highest share price. There is no such thing as constitutional democracy in the world of Facebook and Google.

It is not only a matter of a few consumer markets, but of aspects of life that are important in terms of fundamental rights. There is no longer any distinction between commercial and private activity, between public life on the street and one's own home. Corporate groups are setting about making decisions about everything at their own discretion: whether and how rights or public security are enforced, or in what manner we will co-exist in solidarity. All this would take place without written rules, without any democratic decision-making process and without independent courts. What is taking place is nothing more than a clearance sale of our rights.

Those on all sides of the debate about political challenges have been passing the buck for years, instead of working on proportionate rules for the digital era and then enforcing them, even in the face of the interests of large corporates and lobbyists. Happily, when it comes to data protection we are in the throes of doing just that throughout Europe, although everyone needs to be even more committed in order to achieve a successful result. There are clear indications that data protection is on the agenda as regards copyright reform and enforcement, where it has been possible to remove private processing and the exchange of personal information from the scope of the rules. As in the case of data protection, the enforcement of copyright in the private, non-commercial sphere would not only be excessive, but given the volumes involved in private data processing, it would quite simply be unachievable. At least, this would be the case if we want to avoid full surveillance of everyone's private communications. Instead, copyright needs to be strengthened where it is needed, namely to protect the copyright holder from industrial exploitation and criminal infringements of rights. Although I keep harping on about them, companies such as Facebook and Google need to be seen as uninvolved third parties. They earn their money by disseminating content way beyond the everyday boundaries of private life. Their content is more or less an advertising medium. We need a debate that looks at both sides of the argument, in the hope of finding pragmatic solutions. We must now push for a digital social contract, which strikes a balance between

the justified concerns in the form of properly formulated aspirations and rights in the digital era, during a democratic debate and decision-making process.

The networked society must be capable of carrying its core values forward into the digital era during an open debate. This represents a real challenge for data protection. In contrast to copyright law, data protection involves few commercial interests in strong self-determination among consumers, whereas the economy, government institutions, the media and politicians all have a keen interest in evaluating people's data in great depth. The fundamental right to informational self-determination is thus the toughest and most important conflict among people about their freedom on the Net. It represents the litmus test for the Net movement, and with it, for the civil society of the future.

Following the revelations of Edward Snowden and the debate about the virtually endless data gathering and the wholesale and groundless surveillance of our communications, this has become obvious even to the Net movement. There has essentially been no »Net movement« since the Snowden affair. Since then, there has been such a far-reaching debate within society about the technical realities of our time and the risks of challenges such as digitalisation, that the players in the traditional Net movement, who were previously seen as avant garde, are suddenly surrounded by all those who previously held the view that such topics were not particularly relevant

to politics, the economy and everyday life. All of a sudden, these questions have become the subject of top level discussions and have become the focus of attention in the media and in the public arena.

However, questions are arising that call for a significant amount of self-criticism on both sides: how can we find and enforce the right rules to enable us to coexist in the digital era? Is it even possible to guarantee the security of fundamental rights, the constitutional state and democracy on the Net? These are questions that others had already asked themselves, including those whose viewpoint opposes that of the »Net movement«. The debate about a »Germany Net« or a »Schengen Net«, in the light of the NSA affair, triggered a debate with the potential to escalate, about the »Balkanisation« of the Internet where, ultimately, borders would again be drawn through the global World Wide Web that had just been achieved. In contrast, technical and economic decentralisation was again enforced, to offer better control to individuals and those sectors of society that were able to agree on common rules. Entirely new challenges are opening up for the Net scene, which had formerly been concerned primarily with its own questions and ideas. It must face up to the social conflict associated with its transformation into a fully globalised and digitalised era.

Interesting spokespersons, such as Sascha Lobo or the Belarusian Evgeny Morozov, made their feelings clear in the debate on these questions that was conducted

in German: When recovering digital sovereignty and enforcing fundamental rights and freedoms on the Internet, a serious examination must be made of the power structures of those who have economic, infrastructural and political influence. The ideology of the good Internet, as Morozov rightly reminds us, kept us blinkered for years about the fundamental imbalances and difficulties in the digitalisation process. We will only be able to take the right steps towards common core values for a future digital society if we are able to grasp and name the underlying logic (profit-hungry market players and security-obsessed heads of state). This must take place as a matter of urgency, and the courageous action taken by Edward Snowden will now make it possible for a new generation of digital natives to create these values. Without doubt, every opportunity has its own time window. If we don't manage to take advantage of today's time and opportunities, we will lose much of what we have achieved as we move towards tomorrow's networked society.

A digital declaration of independence

Data protection legislation already had a 40 year history when the EU Commission instigated the process for a fundamental reform of data protection law in the European Union in 2010, on the initiative of the newly created Directorate General for Justice. Data protection law had come into force in the form of an EC Directive 15 years earlier, in 1995, and has since standardised the fundamental principles of data protection in all Member States. This was preceded by fierce debates in the European Parliament and the Council of Ministers. On the basis of a Council of Europe Convention dating from the Eighties, they established common rules for the EU Single Market. Those involved were very likely unaware at the time precisely what they were setting in motion with this Directive. Since its instigation, the EC Data Protection Directive has not only formed the basis of all European data protection legislation, it has also acted as a model for a whole series of third countries. Many countries around the world have since based their own legislation on the European data protection law system. The adequacy checks by the EU Commission demonstrate how the principles of the Data Protection Directive influence the legal systems of other countries. Since 1995, Europe has been a proper exporter of data protection. However, the current debates about the revelations by Edward Snowden and the associated question of the ongoing differences between the data protection rules around the world eclipse this finding. Both

the Safe Harbor Agreement with the US economy, and the application of fundamental legal principles of the EU Member States during business dealings with third country undertakings that process the data of European citizens and from the EU Single Market, are being openly called into question and reconsidered. How can we handle the digitalised world if fundamental legal principles and common standards in relation to fundamental rights can still not be effectively enshrined in law and enforced?

Edward Snowden has suddenly presented us with an outrageous picture of the state of our democracies – a dystopia, the extent of which no-one could have imagined possible. Former exponents were derided as conspiracy theorists and tinfoil hat wearers. But now we know the truth: secret services and Internet giants are burrowing their way through our entire lives. For the link between humans and information technology is by now permanent and automated. We are constantly transmitting information disclosing our personal details. As our proficiency and rules currently stand, very few of us are able to control or prevent this. We are losing just what the *Bundesverfassungsgericht* (German Federal Constitutional Court), almost exactly 30 years ago, described in its judgment on the census as »informational self-determination«, as an expression of human dignity and the right to privacy: a human right that is the basis for the free development and activity as a self-determining citizen and consumer within a democracy.

Unfortunately it is now primarily politicians involved in foreign affairs and security who must deal with the consequences of the current scandal, although they are not concerned with the self-determination of citizens and consumers. With their limited horizons, they only see the diplomatic conflict between government institutions. For them, espionage is the internationally recognised means of protecting ourselves in the international arena, beyond the guarantee of democracy, citizens' rights and the rule of law given under domestic policy. The heads of government vigorously maintain that the insane programmes of the American NSA *(National Security Agency)* and the British GCHQ *(Government Communication Headquarters)* involve spying abroad to counter external threats. The BND (German Federal News Agency) actually justifies its escalating surveillance on the basis that the Internet is quite simply »abroad«. In its view, it does not matter whether we are somewhere in Afghanistan talking to the Taliban on the phone or at home posting something on a friend's Facebook page. The inverse argument reveals the true extent of this dangerous development: our own laws don't apply abroad. For secret services, only the rules of international law apply in the digital world, while for Internet giants, only the vague provisions of the international market apply. We ourselves are transformed from citizens and consumers to combatants and products. Under this interpretation of the law, no legal violations are taking place. In fact it has long been impossible to bring legal violations to court and prove them. As a result, we have

not only surrendered control over our data, but also any influence over the rules relating to their processing.

There is one principle cause for this aberration: when the digital world was created, no accompanying set of social values was created. Unfortunately, politicians never took seriously what the rock texter and intellectual John Perry Barlow described as early as February 1996 as a »declaration of independence by cyberspace«. The Internet, initially occupied by early freedom-loving computer specialists and nerds, has gradually been commandeered at will by governments and corporate groups. It was principally the US Government and Silicon Valley, the latter highly subsidised by government money, for example from the military and the secret services, that systematically and for years fought the battle for supremacy in the digital world. Meanwhile, the digital revolution in Europe missed out, because the US states all carried on with total disregard for everyone else. Firm joint action was impossible for many years. Germany in particular regularly applied the brake when it came to laying down rules for the digital world that would apply throughout the EU. Instead, relatively modest amounts were invested in the development of today's digital economy. The current attempt to counter US dominance by establishing a Deutschlandnetz (Germany Net) follows the same tradition. Instead of taking up the fight for the competitiveness of European companies in the digital market and defending the common values of the EU when it comes to negotiations with the USA, we are get-

ting involved in a symbolic nationalism which cannot, in the final analysis, bring about a genuine reversal of the situation.

It is about time we did one thing in particular: unite Europeans in the battle for fundamental values on the Internet and fair competition in the digital market. What we need is a digital declaration of independence, that upholds the constitutional state, citizens' rights and democracy even in times of globalisation and digitalisation – a digital declaration of independence that gives citizens and consumers back their control and self-determination as defined in the European model, while simultaneously offering European companies an equal opportunity in the digital market. This is precisely what the latest European Union General Data Protection Regulation is seeking to achieve – a common digital market, open to all and offering the same opportunities, and which gives citizens and consumers mandatory high standards. This will not involve compartmentalisation or restriction, but the creation of an open playing field, on which reliable rules apply to all, irrespective of the origin of the companies, authorities, citizens and consumers involved. The fact that in mid October 2013, the European Parliament took a clear stand in favour of joint EU data protection, supported by all the parliamentary parties, represents a great success. It is therefore all the more disappointing that the heads of government, and especially Angela Merkel, have not followed up their fine words about the need for European data protection rules by taking any action. The Data Protection Regulation would be the first step

towards gaining independence from Silicon Valley and would achieve two things: the creation of jobs on the European digital market and the defence of the European standards of data protection and consumer rights.

Silicon Valley has a design fault that is difficult to rectify, because the US Government cannot now keep control of the Internet giants that it brought into existence as garage start-ups. Under US law, Facebook, Google and Co. may operate with virtually no legal and geographical limits. The technology and services that they generate need not meet any of the fundamental prerequisites of the social environment and have by now taken on an essential role for politics and government alike. The lobbying they fund is the most expensive and unquestionably the most influential in both Washington D.C. and Brussels. To disempower them, Europe would have to close a digital new deal over the long term, offering huge investments to the European Internet companies while imposing the European values and rules on them. A fairer deal between between citizens, the government and the Internet economy must make one thing clear, to the latter in particular: we are investing in you so that you will be able to survive on the market as a counter-model to Silicon Valley and to stand for self-determination and regulation in that market! However, this takes political courage, coupled with a renunciation of an inward-looking policy in Germany, which is concerned only with German rules and German debates. Instead, German policy (in the digital field in particular) must ultimately become the driver of strong EU policy.

As regards data protection as the most important pillar in this conflict, politicians must finally appreciate the fact that it is no longer possible to simply narrow the consequences of mass data gathering to rudimentary consumer protection on the Net and better control of the security authorities. There is a far wider dimension to the situation: Compared with the analogue world, when it comes to the data gathering of the Internet and telephone providers, insurance companies and banks, marketing firms and online shops, the providers of smartphone apps etc., it is as if a host of spies and analysts were sitting at every crossroad, in every tree, doorway and room, who would simultaneously write detailed reports on each of our lives, archive them for eternity and make them available to virtually anyone in the blink of an eye. And for those who believe that the problem will be solved if the NSA or the secret services are all put in their place: it isn't NSA spies and analysts who record it all, it is the companies who develop and offer us the products and services. The NSA and many others simply access the data. This does not make things better. However, it does show that we really do need an enforceable fundamental rule that finally gives us back control and sovereignty, as self-determining people, over the true data gatherers of the private sector. To achieve this, we need a digital declaration of independence. The EU data protection reform would be one of the central building blocks for this, and it is within our grasp.

An effective regulatory framework for data protection throughout the EU market would represent the greatest step towards true consumer independence. Instead of abandoning the Internet and technical progress, all consumers (including those outside the EU) could as a result claim control over their own data in Europe legally and backed by sanctions, and only make them available to those who provide them with a high level of protection and who make sparing use of data. People could decide themselves whether they wish to take the risk of transferring their data to a cloud server in India, where the legal situation as regards the fundamental rights of those concerned could differ. They could also ensure that there is a financial incentive for companies and an economic incentive for their governments to insist on technological and effective data protection security. In this way it can suddenly make sense for governments to promote the fact that they will essentially maintain the protection of anonymous communication, encourage encryption and only allow identification in certain specific, regulated circumstances. And it will suddenly make sense for companies to submit to an independent audit in order to detect any data protection and security loopholes. However, if we are to take this step towards a new way of handling data protection, we need courageous politicians with the political backbone to break new ground.

Data protection reform in Europe

At the end of January 2012, the European Commission proposed an eagerly anticipated reform of data protection law. After a substantial consultation process, this reform is a major step towards comprehensive legislation on data protection throughout the European Union and, to some extent, even beyond it. The new EU law could bestow great benefits, particularly on users of Facebook and Google or smartphone owners, because up to now, they have in practice enjoyed hardly any protection against having their data stolen and sold to third parties. In an era when many personal data are no longer processed in the data subject's own country but are increasingly processed on the Internet, the fragmented legal situation which exists is no longer appropriate. The existing data protection laws are inadequate. Businesses are hardly required to account for their use of personal data, let alone having to fear any consequences. They make self-assured inroads into the market with the new functions built into their products, which process yet more data in new contexts. Those who are in any case using their products or services often have no choice. Who actually wants to give up a Gmail account that he or she has been using for years just because they do not agree with a new ›feature‹, such as linking of search terms and e-mail usage data in order to ›optimise‹ search results? The legal situation that currently applies, governed by the EU Data Protection Directive of 1995, was established at a time when many of these

aspects were not yet relevant in any way, as the internet was then in its infancy. The basic rules of the Directive are not wrong on that account, and what is needed is not to reject them but to enforce them more effectively and elucidate their principles as they apply to the digitised world of today. This is where the EU should act, and where it has proposed to do so, thereby opening a new chapter in the laying down of international data protection rules.

The proposals for a fundamental reform of European data protection law are intended to provide consumers and citizens with a uniform EU standard for the effective protection of their data. In addition to increasing the ability of individuals to receive information and exercise control, the intention is to introduce tangible penalties that will apply in the event of abuse, such as the loss or resale of data. In view of the deliberate manner in which data collection companies around the world contravene data protection legislation, such a step is already long overdue. Yet even at the drafting stage of the Commission proposal, some vital demands fell victim to the interests of big businesses and security authorities.

The influence of the lobby of major IT businesses from Silicon Valley and the powerful advertising industry made its presence felt from the outset. For example, as soon as the reform debate began, former Minister of the Interior Hans-Peter Friedrich (CSU) announced that voluntary commitments by industry

were sufficient and that there was essentially no need for stronger European data protection. This is despite the fact that Germany of all countries ought to have been lobbying in Brussels for a strong EU-wide data protection standard, as the Federal Constitutional Court had, for years, been formulating a clear fundamental rights standard for data protection. The European internal market and the massive exchanges of data between both businesses and authorities throughout the EU have undermined this standard for years. The case-law of the German Constitutional Court also has an impact on the EU's international law in this context. Since the Lisbon Treaty, which entered into force in the form of the EU's new ›Constitution‹ on 1 December 2009, the fundamental right to data protection has not only formed an element in the binding EU Charter of Fundamental Rights but also a central principle of EU law. Throughout Europe, data protection is a fundamental right which the State must protect – against State authorities and private businesses alike.

What the European Commission's new proposals mean for consumers and citizens is, above all, greater transparency and control over their data. In the case of everyday applications and services, which are storing more and more of our information, it is intended that deletion and correction should become significantly easier in future. The Commission proposal is therefore a good starting point in principle. It aims to secure high standards of data protection which are more har-

monised and appropriate to the internet age, while retaining the fundamentally worthwhile principles of the 1995 Directive: data minimisation, the consent of the data subject, a requirement to confine the use of data to the purpose for which they were gathered, and a right to information. From the point of view of civil law, the primary concern is to limit the number of exceptional rules that apply and to lay down the good ideas in specific terms. The new ideas would also represent a major benefit for the local economy. But, for businesses here too, the new rules would represent considerable progress, because at present they have to comply with 28 different sets of data protection rules in the EU's common internal market and thus, despite much bureaucracy, enjoy absolutely no legal certainty. Moreover, they have to compete with internet giants from Silicon Valley and other data gatherers who employ armies of lawyers to look for loopholes in this obscure jungle of rules, so that they can often evade the regulations. They were up in arms against the new rules because many of them make good money by exploiting the loopholes and inadequacies in data protection law in its current form. They have also enlisted massive lobbying assistance from the US Department of Commerce, which has long regarded European data protection as a thorn in its side.

In the context of the reform of data protection law within the EU, which has been ongoing since January 2012, Europe has the opportunity to transform those regulations into a worldwide gold standard. Politicians,

businesspeople and nongovernmental organisations – across the political spectrum – consider that a reform is needed. Everyone must regain control over their own personal data, these being the currency of the digital economy. Like any other currency, it needs confidence in order to be stable. The revelations concerning eavesdropping on data by the secret services have shaken confidence not only in transatlantic relations but also in the digital economy. Members of the public are not the only ones to be concerned. Gathering, exploiting and transferring personal data also creates an enormous economic potential: in 2011, the data of EU citizens were worth € 315 billion, according to research findings. However, people will no longer disclose their details if they do not trust the businesses that are going to process them. Loss of confidence translates into loss of revenue. Data protection reform will help to restore confidence. The citizens of the Union wish to be certain that, in disclosing their personal data, they are not renouncing their rights. In addition, reinforcing the high standards for data protection that apply in Europe will also require new commercial prospects to be created. In that regard, data protection will become a sales argument and a competitive advantage.

In the meantime it has become clear to everybody that we can only acquire control over our data by means of an EU-wide guarantee, because in the digital era, information is no longer confined inside the boundaries of states, let alone regions. For a long time already, commercial groups, undertakings and authorities have

all been exchanging large quantities of information across borders or are already working entirely in the *cloud*. The European Commission proposal was therefore a good basis for linking a stringent data protection standard to a substantial increase in legal certainty for businesses, authorities and consumers, and was sorely needed: the 15-year-old framework data protection provisions in the EU cannot confer lasting protection on personal data. In the European internal market, it is unfortunately the country with the weakest data protection law that sets the standard. The European Commission was therefore right to seek an EU-wide set of provisions which would replace large parts of national data protection laws and require cooperation among data protection officers. However, this will make it all the more important to set the bar high and make retrospective improvements where the customary level of protection could be reduced in the Member States.

After being submitted in January 2012, the Commission proposal was forwarded to the two branches of the EU's legislative authority – the Council of Ministers and the European Parliament – since when it has been debated by the appropriate specialist committees there. Only once both sides have a negotiating mandate can a common position be arrived at under the EU's legislative co-decision procedure. It was originally intended that negotiations between Parliament and the Council should be held in spring 2013, but the adoption of the negotiating positions was delayed on both sides. On 21 October 2013, after more than a year and a half of nego-

tiations, the European Parliament reached agreement on a mandate for the consultations with the Council. Following many rounds of negotiations and after no fewer than 3 999 individual amendments had been tabled, a broad majority within the committee responsible, the Committee on Civil Liberties, Justice and Home Affairs, had agreed on a compromise text which modified virtually every article in the Commission's draft, but which clearly endorsed the proposal's basic aim of establishing a uniform body of EU data protection law. Since then, Members of the European Parliament have been awaiting the beginning of the negotiations with the Council. In adopting its own position, Parliament had called on the Council to come to the negotiating table quickly so as to enable a first reading to be held without delay and allow the data protection reform to be adopted before the European elections in May 2014.

However, this did not come to pass, as the Ministers of Home Affairs and Justice were unable to agree on large parts of their reform for over three years after the publication of the Commission proposal, Only in March 2015 the Council was able to arrive at a position of its own on the data protection regulation. How could this happen? Since the Commission submitted its proposal at the beginning of 2012, government representatives in the Council have taken the talks into one extra round after another because some Member States – particularly the UK and Germany – have been delaying the negotiations by means of innumerable discussions of matters of principle. Despite some fruitful

discussions, most of the issues were brought forward to please the Big Data industry, watering down the principles of data protection. This led to some positions of the Council being criticised as going even below the level of protection set by the Directive 95/46/EC. During the ongoing trilogue negotiations this is being heavily discussed.

From the outset, the European Parliament was the driving force behind EU data protection reform. Even in the years before the Commission proposal, Members of the EP had intensively debated protection of citizens' data in the digital age when discussing the US authorities' access to data from the bank service provider SWIFT and passenger data held by airlines. Uniform EU data protection law had already frequently been called for at the time, as it had repeatedly emerged how incomplete protection was in the EU and in relation to third countries. In its original resolution on data protection reform, the European Parliament had already made better enforcement of EU data protection law in the common internal market one of its main demands, in which connection it particularly had in mind businesses operating on the EU's internal market from third countries. In the course of the ceaseless development of the digital market and the opening of the internal market for businesses from third States – particularly by means of the Safe Harbour Declaration for businesses from the USA – it had become increasingly clear that the supervisory authorities of the EU Member States had problems in enforcing data protection law. In most cases it is not

the data protection authority of our own country that is responsible for protecting our data at all but that of a different EU State entirely, because it is there that businesses have their establishment within the EU market. Often, this results in protracted coordination processes between supervisory authorities, not uncommonly ending with the finding that the 1995 Directive has simply been enforced very differently in the Member States, and that in practice enforcement measures still vary enormously between supervisory authorities. In view of the importance attached to data protection as an individual fundamental right, the vast majority of Members of the European Parliament have taken the view that this is unacceptable. Their call for the European Commission to propose a uniform data protection law with uniform application and enforcement could not have been expressed more clearly. Moreover, the European Parliament has called for such uniformity not only in relation to the EU Member States but also with reference to the various fields of law and application. Paragraph 6 of its resolution of July 2011 also read as follows:

> *›The European Parliament considers it imperative to extend the application of the general data protection rules to the areas of police and judicial cooperation, including processing at domestic level, taking particular account of the questionable trend towards systematic re-use of private sector personal data for law enforcement purposes, while also allowing, where strictly necessary and proportionate in a democratic society, for narrowly tailored and harmonised limitations to certain data protection rights of the individual‹.*

This made it clear that the European Parliament was calling for horizontal regulation at EU level and wanted to allow any departures from it in Member States' legislation only in exceptional cases. The European Parliament decision and also the feedback both from the consultation exercise and from the Member States quite clearly had a big influence over the formulation of the Commission's legislative proposals. In January 2012, when the Commission submitted its proposal for an EU General Data Protection Regulation, the feedback from the European Parliament and from European data protection experts was fundamentally positive. This was despite the fact that, even during the internal coordination process, some proposals by the Directorate-General for Justice had required modification, such as the requirement of a legal basis in EU law for a transfer of data from the EU to third-country authorities. These were deleted in response to pressure from other directorates-general, which had very obviously yielded to strong influence from the US Government. This was a foretaste of the altercation which was to be anticipated with lobbyists representing Silicon Valley, who had by now become powerful, indeed possibly the most powerful lobby group of all, and had already been testing the resilience of regulators on both sides of the Atlantic for years.

It is quite clear that the proposed reform does not constitute a substantive revolution and was never intended to. It largely and above all extrapolates from the existing right to data protection with its fundamental definitions and principles.

As a result of the proposal, a lively debate sprang up among experts, although in many cases it was very far from comprising a constructive discussion of the Commission proposals and from expressing a desire to improve them. As so often in the case of major steps towards integration, the harmonisation of data protection too involved the issue of subsidiarity and compatibility with the existing national legal framework. However despite the debate about the consequences of full harmonisation through an EU regulation, almost everyone realised that there was no alternative to greater harmonisation of data protection and common case-law at EU level. Furthermore, all those involved agreed that therefore a democratic process of setting single standards for the EU single market was the only way to get legal certainty, a level playing field and a starting point for international standards in the digital market.

After I was appointed as the European Parliament's rapporteur on the EU data protection regulation in March 2013, the talks began with the Members responsible from the other political groups and with the numerous stakeholders, on the possible position to be adopted by Parliament on the specific proposal by the Commission. As the European Parliament's rapporteur, I am one of the Members who has the greatest influence on the Regulation. The onslaught which I experienced in the following year was correspondingly massive. Subsequently, I published on my website a list of the people whom I met during this period leading up to the presentation of my draft report (constitut-

ing the basis for deciding Parliament's position) in January 2013 with the aim of reflecting the various points of view in our work. In addition to the many meetings with colleagues within Parliament and representatives of the European Commission and Member States, I met nearly 200 different stakeholders during this period alone, some 90 percent of whom were from the commercial sector. This more than clearly demonstrates the significance that our personal data and the data protection regulations have nowadays in all spheres of life, and it has also shown how strong and how one-sided the often invisible influence exerted by strong lobbying groups can be. A few large IT groups, particularly from the USA, conducted a massive lobbying campaign in Brussels and Strasbourg, investing large sums in lobbyists of their own and in numerous associations, consultancies and firms of lawyers. This enabled them to provide not only me but the more than 750 other Members of the European Parliament and anyone else involved in the reform with ample information about their positions and arguments, while it was often not clear to members of the public that the future of their fundamental right to data protection was being negotiated here.

Once I had presented my draft report for the position of the committee responsible – the Committee on Civil Liberties, Justice and Home Affairs – the other Members had the opportunity to table their own amendments to the Commission proposal. In addition, four other committees which had been asked to

deliver opinions decided what their positions should be and contributed them to the procedure. By the time of the deadline for tabling amendments in March 2013, the European Parliament had 3 999 amendments to consider. As the rules require, all of them were translated into 23 official languages and suddenly appeared in huge stacks outside our committee meeting room. Never before during the legislative procedure in the Members' chamber in Strasbourg had so many requests for amendments been submitted. As rapporteur, I had to fulfil the virtually impossible task of formulating compromises with the coordinators of the other political groups on the basis of the amendments tabled, the aim being that, when it comes to the final vote, a majority of Members would support those compromises. Fundamentally speaking, Parliament had from the start been fairly unanimous about the data protection regulation. It welcomed the Commission's proposal and, together with the Commission, urged that the proposal be adopted quickly with a few clarifications. The original aim was to reach agreement before the end of the parliamentary term, meaning before the European elections in May 2014. However, the reform was repeatedly delayed. Both in the Council of Ministers (a point which I will discuss in detail below) and in Parliament, massive lobbying influence made itself felt from the outset. Large IT groups such as Google, Microsoft, Amazon, Facebook and IBM are precisely the ones that invest the most in lobbying: both in Washington D.C. and in Brussels they spend

many millions every year with the aim of bombarding decision-makers with advisers, lawyers and events of all kinds, while attempting to conceal and camouflage this influence as best they can. Some undertakings simultaneously support several different lobby groups, think tanks and ›civil society‹ initiatives in the area of data protection and the free movement of data, in order to increase the number of reiterations of invitations, lines of argument and position papers. By means of *›astroturfing‹*, they seek to use other groups (for example small and medium-sized enterprises, which are exploited by large companies in just the same way as consumers are) to promote their interests or even pretend to be speaking on their behalf. At many meetings with various stakeholders, I heard certain statements and arguments, some of them distorting and tendentious, again and again, put to me in virtually the same words, although the groups had actually approached me expressing quite different concerns. Things became even more absurd when lobbyists acting on behalf of big businesses did not even mention their own interests but vehemently advocated the alleged interests of consumers and then told me that the latter actually did not want data protection at all. On the contrary, people were happy to give businesses their data and did not want to be consulted as to whether anyone should be allowed to receive them. Consumer protection organisations, with their totally inadequate resources, which contrary to this depiction described consumers' interests quite differently – and in my view

far more accurately – often did not even succeed in reaching Members of the European Parliament with their arguments. Members' diaries were already full of meetings requested by industry lobbyists. The massive pressure which was brought to bear by these lobbyists from the very beginning of this legislative procedure became clear in the summer of 2013, when the website LobbyPlag.eu showed that hundreds of amendments tabled by Members in the European Parliament had been copied word for word from position papers or amendments formulated by large internet businesses. LobbyPlag.eu had drawn up an overview of all the position papers of big businesses and lobby groups of all kinds and compared them with the hundreds of amendments tabled by Members of the European Parliament. After this, some Members vehemently disowned their own amendments, as the public took exception to their having acted so one-sidedly on behalf of large IT businesses, thereby opposing consumers' rights. The former EU Commissioner and current Member of the European Parliament representing the Belgian Liberals, Louis Michel, even dismissed a member of his staff, accusing him of having tabled hundreds of pro-industry amendments in his name without his knowledge or consent.

The debates at the European Parliament nonetheless proved highly productive. In the course of more than 50 meetings, it was possible to draw up a strong compromise text with the agreement of all the political group coordinators and with the assistance of many

members of staff, which was adopted by an overwhelming majority in Parliament. The question which arose again and again was what data protection rules were needed in order for people to gain control over the disclosure and use of their data. Data protection begins even before a service is used. Users need to be unambiguously informed what will happen with their data in order then to give their informed consent. But hand on heart: Who actually reads the many pages of General Terms and Conditions pertaining to the internet services they wish to use? What is needed, therefore, is simple and readily comprehensible conditions of use in the form of standardised symbols, comparable to those which exist for food. The ideas put forward in Parliament ranged from a data protection traffic-light system to quite detailed descriptions of all intended uses and methods of use. In the end, Members opted in their negotiating position for a statement of the basic rules of data protection law and marking to indicate if data are to be transferred to third States. In addition, there should also be technical ways in which users can defend themselves against the use of their data for certain purposes by means of a standard setting: if the privacy settings of a browser indicate that the creation of user profiles has not been consented to, service-providers should respect this. One way of implementing this would be by means of the Do-Not-Track function, which is already installed in widely used browsers, but does not really function as yet. The proposed legislation should now change this situation.

On the side of the undertaking too, data protection begins before a service is offered. The reform proposal obliges businesses to design their services in such a way as to minimise the amount of data required, with pre-settings which promote data protection to the maximum. Facebook, for example currently operates in precisely the opposite way: if I open an account, the default privacy settings are the lowest available, and if one wishes to change the settings, one is confronted with explanations which are extremely challenging. In encouraging design with built-in data protection, we aim to apply the principle of purpose limitation more thoroughly. In other words: what data are genuinely needed in order to use a service? And: is it always necessary to identify me beyond all shadow of a doubt? These are questions that service-providers should put to themselves in advance. Many services also work if used anonymously or using a pseudonym. Whether my girlfriend chats with me under her full name or as ›spacecommander86‹ does not in any way affect our communication.

Once our data are out in the world, it is important to retain control over them. Retention periods must therefore be clearly defined, and data must be deleted again once the purpose for which they were to be processed has been accomplished. It must be easy to exercise and apply the right to deletion and correction which is enhanced by the reform proposal. The debate concerning the ›right to be forgotten‹ which the European Commission has proposed, played a central role here,

a right which Parliament regards as part of the right of deletion and therefore no longer mentions separately. This is not a matter of technical expiry dates or indeed erasers but a legal right to secure compliance with a request for deletion. A provider who, without my consent, has gathered data about me, passed them on or published them should also seek to induce third parties to comply with a demand which I have made for correction or deletion. People whose personal information from their youth has unlawfully been communicated over a social network have an interest, quite rightly, in ensuring that, ten years later, their job opportunities or their chances of obtaining a mortgage no longer depend on it. This of course does not apply where a public interest is at stake or where there are issues of freedom of information and opinion. The aim is not to give politicians, for example, a back-door method of preventing unwelcome reports from being published. Rather, the purpose is to reduce the impact of the unlawful processing/reprocessing of data.

To this end, the Regulation ought to strengthen rights to information vis-à-vis providers. I should be informed in intelligible language, free of charge and as quickly as possible, who is doing what, using which of my data. Another innovation is the right for individuals to receive their own data in a common electronic form: at my request, service providers should divulge to me the data which they hold concerning me, in machine-readable format, i.e. digitally and not in the form of hundreds of pages. This would then enable me

to switch to a competing provider that is more favourable with regard to data protection or to be able to view my data.

In order for the Data Protection Regulation not to remain a paper tiger, the proposal for a regulation aims above all to improve enforcement of data protection law. For this purpose, the first step is to give data protection authorities more power. Data protection who? Only one third of people in Europe are aware of their national data protection authorities. These are normally responsible for monitoring and enforcing data protection standards, and so far their powers have not extended beyond the national borders of the Member States. The reform proposal is therefore intended to improve cooperation between national data protection authorities, so that my national data protection authority, which speaks my country's language, will always be my contact. What this requires above all is for data protection authorities to be better equipped. The reform proposal also calls for financial penalties equivalent to 2% of businesses' annual turnover – indeed, in its decision the European Parliament even increased them to 5%. Penalties on this scale can cause pain. As a comparison: the supermarket chain Lidl was recently fined € 1.5 million by the data protection authorities for infringing data protection rules. However, Lidl's annual turnover is € 30.85 billion: if the cautious Commission proposal were to be applied, the business would have to pay € 617 million – 411 times as much.

The cornerstone of the Commission proposal was the so-called consistency mechanism, which, in conjunction with the ›one-stop shop‹ principle, should create a win-win situation for us citizens on the one hand and for data processors on the other hand. Every processor who falls within the scope of the Regulation will have a fixed dialogue partner in the form of the data protection authorities in his own EU country and will no longer have to argue afresh about the same issues with the authorities in each country. In addition, the inconsistent implementation and application of data protection law is finally to be consigned to history by enhanced, binding cooperation at EU level, thus, for practical purposes too, giving citizens a fundamental right to data protection which can be permanently enforced. This was also the approach which Parliament had very clearly espoused even in advance of the Commission proposal, by focusing on enhanced cooperation in the Article 29 working group. In its negotiating position, however, Parliament opted for a slightly different approach to that of the European Commission: unlike in the Commission proposal, Parliament was against giving the last word over a dispute within the newly created European Data Protection Committee to the European Commission, and instead favoured empowering the supervisory authorities within the committee themselves to take the decisions which were to bind them. This will preserve the autonomy of data protection authorities and at the same time guarantee coherent application of data protection law.

The revelations by Edward Snowden in the summer of 2013 evoked at least one direct political response: in the European Parliament, a broad majority of Members soon backed the reintroduction of the former ›Article 42‹ which had figured in an internal preliminary draft of the Commission, which Parliament's rapporteur had reinserted as a new Article 43a. This clause stipulates that the transfer of personal data from the EU to third-country authorities is only permitted on the basis of European law or of mutual assistance treaties based on it. This would mean that the transfer of data, for example by telecommunication or internet undertakings, to the security authorities of third States would be explicitly prohibited by the EU's General Data Protection Regulation so long as there was no agreement with the EU on cooperation in this field.

Although a large majority of Members of the European Parliament were in agreement on many of these points from the outset, the procedure took significantly longer than planned before a negotiating position was agreed for the final negotiations with the Council. The original plan to vote on my report in April 2013 was impossible to adhere to after the deluge of amendments had arrived. The postponement of the vote, initially until the summer and then the autumn of the same year, was due to the complex and detailed discussions between the political groups with a view to reaching compromise formulations for each individual article in the Regulation. Only in that way was it possible to ensure that the whole procedure would conclude with a result

which would be internally consistent and genuinely supported by a broad majority of the political groups in Parliament. However, ultimately the big interest being taken in the work on the General Data Protection Regulation also shows that data protection has taken centre stage in the political debate and is now relevant to all areas of life and the economy. Members of the European Parliament know very well that many members of the general public are monitoring their work on this regulation. It was therefore right to make the debates in the European Parliament as public as possible. Numerous hearings were held in 2012 and 2013, and the coordinators from the political groups and I, as rapporteur, each attended hundreds of events dealing with the various aspects of the data protection reform in parallel with the already very packed calendar of meetings of the European Parliament. Unfortunately, however, in the EU's legislative procedure this is not enough to give people a complete overview of what the main aspects and controversial points are and who is adopting what position. Because on the other hand, there is the Council, with its power of co-decision, whose structures to this day – despite the massive importance of the EU to us all – are built upon diplomatic negotiations behind closed doors, at which the participants themselves feel little burdened by any duty of public accountability for the outcome. It is still the case that the governments of the EU Member States act as if EU decisions were based not on their actions but on the work of an impenetrable bureaucracy in Brussels. In any event, this

is the picture they like to present when the decisions taken are assumed to be bad or undesirable. If, on the other hand, decisions manifestly and immediately appear valuable to people, the way that governments prefer to present them in the EU capitals is still as if the individual government had dreamed the whole thing up itself and managed to persuade other Member States to support it along the way.

That is why, within the Council, some EU Member States can take the liberty of rejecting certain European Commission proposals not on account of a substantive consideration of the proposed legislation but because they are critical of the EU as a matter of principle or simply because they do not wish to accept proposals which they have not devised themselves. This, regrettably, has also happened with the Data Protection Regulation. From the outset, the discussions within the Justice and Home Affairs Council were marked by fundamental criticisms by the British, Danish, Hungarian and German Governments, while such Member States as Spain, Poland, Portugal, Austria and Ireland urged that the Regulation be dealt with and adopted quickly.

The reform was particularly obstructed by the persistence of those who had accommodated themselves to their existing situation. Particularly on the part of the Member States, there was a strong tendency towards fearful rejection because authorities, judges and politicians saw the proposal as jeopardising the role which they had played in data protection to date.

In addition, their fears were repeatedly exploited by certain quarters, which in their turn were influenced by other extraneous or concealed interests, to agitate against the reform proposal. In the negotiations within the Council, it sometimes became clear that some government representatives and ministries, while hiding their hands, were guilty of false play. One of them, unfortunately, on many an occasion, has been the German Government, whose representatives quite clearly regarded the EU reform as a general problem and have tried by every possible means to prevent agreement being reached even on interim results. For months, the German Government questioned as a matter of principle whether the Regulation – and hence uniform EU data protection – should apply at all in the field of data processing by the authorities, and sought to exclude it from the scope of EU data protection law. This was a particularly absurd attitude, given that, since the 1995 Directive, no distinction between private and public data processing has existed any longer for the purpose of data protection principles. There are good reasons for this, because nowadays private-sector data are also – and are particularly – being used for the purposes of the authorities, and authorities also now constantly exchange data across borders. It would therefore be quite ridiculous to exclude the authorities, of all organisations, from the EU's stringent common data protection standard. Moreover, the EU General Data Protection Regulation also provides for a large measure of flexibility in formulating rules on data gathering and data

processing by the authorities. This is something that the European Parliament had expanded upon right at the start of the consultations. In addition, the existing rules regarding the issue as to whether and under what circumstances the authorities are actually permitted to collect data, will continue to be governed by the laws of the individual Member States.

Meanwhile the lobbyists and lawyers employed on behalf of IT companies with international operations celebrate every day that the EU Data Protection Regulation is further delayed by those debates. Perish the thought that Google, Facebook, Amazon and others of course cannot only persuade Members of the European Parliament to table hundreds of amendments which one-sidedly benefit them, but can also get to know many people inside the ministries of the EU Member States and get them on their side. Indeed, it may even be easier there, as the political leadership of ministries is often far more concerned with solving domestic problems than with the protracted technical debates at EU level. In the summer of 2013 – immediately after Edward Snowden's revelations – the German Chancellor Angela Merkel made it clear in an interview that the EU's General Data Protection Regulation was an absolute priority for her. Yet as early as at the meeting of Heads of State and Government a few months later, in October 2013, she backed the British Prime Minister David Cameron when he rejected the request by France and other EU Member States to

see the reform adopted by 2014. The target was then only 2015. However, it is still unclear if this date will be met. Therefore, the envisaged date for adoption became 2015.

Thus the European Parliament was going into the European elections with its negotiating position established and Member States were asked to come to an agreement as soon as possible. It still took them a year to get there. Since July 2015, trilogue negotiations are taking place to finally find a compromise and allow Parliament and Council to adopt the law. If it is not possible to reach a political agreement before the end of 2015, people in Europe will presumably lose confidence not only in effective protection of their data but also in the ability of their politicians to agree on the common rules that people would like to see at European level. This would also jeopardise the legitimacy of the European Union as a whole and the newly won EU fundamental rights. In view of the many data scandals involving either businesses or the State, citizens would resignedly turn their backs not only on the digital market but also on democracy. At a time when precisely this is an enormous problem, it would be fatal simply to allow the window of opportunity for agreement on the EU Data Protection Regulation to pass by. That the opportunity is already passing is clear: the new European Parliament will include a good many Members who in any case will be against any form of regulation at EU level. At the moment, many people are taking a far greater interest in data protection than usual. Yet

with every day that passes without any enforceable EU data protection, the reality of evasion and undermining of existing rules becomes ever more manifest. There is a serious danger that one day we shall look around us and notice that the rules that used to apply are no longer being taken seriously by anybody and that the opportunity to place them on an effective footing jointly with other partners (in this case the EU) in time has passed. The longer it takes for us to establish a new legal framework at EU level, the weaker the protection of our self-determination as citizens and consumers in a globalised and digitised world will be. In the period ahead, it will become clear which way the wind is blowing on the reform of European data protection law. The public debate will be vital, as will a refusal to allow the politicians in whom responsibility is vested merely to play for time and a refusal to accept the claim that in the internet age it is simply no longer feasible or appropriate to the age in which we live to enforce self-determination in the use of people's own data.

You have something to hide

Unfortunately, the old adage that all that glitters is not gold also applies in Europe. Not only in the debate with the powerful economic interests involved, but above all, whenever the interests of the State are at stake, the more effective implementation of the fundamental right to data protection is becoming increasingly difficult. For years now, the interests of State authorities when it comes to maintaining control have created a situation in which the security and surveillance measures have been made more stringent with each step along the road towards the globalisation and digitisation of our lives. In the absence of courageous steps towards integration aiming at the creation of international rules that can be implemented by all (such as for the effective combating of organised crime, tax evasion, money laundering and corruption), politics is aiming to achieve comprehensive checking of individuals, as a means of meeting the new challenges with which it is faced. Conservative and social-democratic Ministers of the Interior in particular are increasingly demanding additional surveillance in order to improve security. They seek to combat cross-border criminality and internet crime by introducing large-scale surveillance. Not only does this contravene people's fundamental rights, but its effectiveness is also questionable. What they are actually saying is that every one of us is a suspect and they are, at considerable cost, constantly creating new information collection measures, body

scanners, video cameras, drones and what are known as »databases of agitators«. At the same time, police stations are being merged and closed down, professional development training cancelled, funding for mobile police street patrols and preventative policing cancelled and several police officers are required to share internet access. The impact of this is devastating. The police is withdrawing further away from public life and is changing to become a force that is now only deployed for the purpose of prevention.

The anti-terror measures implemented in the aftermath of 11 September 2001 and the attacks in Madrid in 2004 and in London in 2005 would not stand up to a matter-of-fact anal ysis into their effectiveness, EU home affairs ministers continue to repeat the mantra that such massive infringements of our fundamental rights are needed, in order to combat international terrorism. The true situation is that in the majority of cases, the processing of foiled attacks and attacks that were carried out is revealing striking shortcomings in the investigative capabilities of the police. Ministers of the Interior regularly use measures involving the comprehensive surveillance of the population as a sort of fig leaf, whenever crime and terrorism create fear within society. Schizophrenic actions: As a means of justifying large-scale incursions into the fundamental rights of individuals, such as by means of data retention, involving the storage of everyone's telecommunications data, without reason and ›just in case‹, national politicians actually go so far as to stoke up that fear even further.

They act as if the internet is a haven of criminality and a lawless space that can only be turned around by retaining large quantities of data. That having been said, the resolution rate that applies to internet-based crime is comparatively high, at 65 %. The German Federal Criminal Police Office has already been forced to admit on several occasions that there is essentially no difference between the rate of resolution that is achieved either with or without the retention of data. Even at the time that the EU Directive was adopted back in early 2006, there had been massive criticism of the absence of evidence of the specific necessity for the retention of data.

Many national politicians no longer seem to be aware of the fact that other types of investigation are available, other than the full-scale surveillance of every single person. It is therefore no surprise that the presumed exception relating to the storage of data relating to individuals not suspected of any crime has actually become the rule. Detecting factors indicative of criminal conduct is not a task that can be carried out by computers and data analysts, which is why we need police officers who have been suitably trained for the types of investigation they are required to carry out. But it is that training that is largely falling by the wayside, even though we actually need those tasks to be carried out, in order to combat crime. The actions undertaken by individuals cannot be predicted on the basis of a calculation. It is a case of working towards a situation, in which globalisation and digitisation will

not give rise to the dissolution of social and human control and in which direct contact with individuals will continue to be the point of reference used by police officers who are good at their job. The more money spent on databases and surveillance technology, rather than in effectively equipping the Police and the judicial authorities on the ground, the further we will move away from that principle. We are constantly seeing important representatives who, either purposefully or unintentionally, ignore the fundamental structures of a constitutional state. The former German Minister for the Interior, Hans-Peter Friedrich, is a politician cast in that mould. His view is that security in the face of crime and terrorism is the most valuable of all civil rights and is therefore a »super civil right«. If we take a look at the text of the legislation, the legal situation becomes clear: no such fundamental right forms part of either the German Basic Law, or the Charter of Fundamental Rights of the European Union. It is the role of the State to guarantee security and the effective combating of crime, but no such individual right exists that is more important than other fundamental rights, or, as Mr. Friedrich clearly believes, has priority over other fundamental rights. In that regard, he is completely wrong. What already exists in Germany, as well as in the European Union, is the fundamental right to privacy and data protection. Any incursion into that fundamental right must be justified and proportional in each individual case. and that is often already the case today, whenever the fundamental rights of others

are affected or under threat. Over a period of many years now, we have developed a body of legislation and case-law that address this essential balance.

What is clear is that the challenges in terms of security and criminal prosecution on the one hand and for the enforcement of fundamental rights and democratic principles on the other are not getting any smaller. What we need is improved cross-border collaboration, together with common, uniform regulations. But anyone who believes that they can move away from important fundamental rules and limits is simply putting wind into the sails of those who oppose democracy and the rule of law. The large-scale surveillance carried out by the US secret-service organisation, the NSA, the secret-service of the United Kingdom, GCHQ, and clearly also by the secret service agencies of other EU Member States forms an unparalleled example of how these fundamental rules can be disregarded. The surveillance and analysis programs developed in secret by IT specialists employed by these organisations, such as *PRISM, Tempora, Echelon, Bullrun* or *Xkeyscore* are disproportionate, as they subject a large number of completely innocent individuals to automated screening and analysis. Secret service agencies are not the only organisations to be carrying out general surveillance work for no specific reason. In the case of the *Secure Flight Program* operated by the United Kingdom, which is primarily based upon an analysis of the *Passenger Name Records* (that is, passenger's details) or the *Terrorist Financing Tracking Program* operated by the US Finance

Ministry, which was »approved« by the EU as a result of the SWIFT Agreement, the police and public prosecution authorities have now gained access to this type of far-reaching methods of the type operated by secret service agencies. This trend has been gaining pace since the fall from grace of the »Echelon« programme, which became public knowledge in the late 1990s: the mass eavesdropping programme for which the Echelon system was used and which involved the interception of almost all telephone calls using a system of satellite-enabled surveillance formed the reason for the convening of an investigative committee in the European Parliament, whose work lasted a number of years. The final report was however submitted only a few days prior to 11 September 2001. That was the reason why the conclusions and recommendations went unheeded, being replaced by the rapid development of technical capabilities and the gradual »breaking loose« of the secret services.

The result of this was that in all of the Member States of the EU at least, data protection and the protection of privacy became a conditional human right. The delusions of the secret services with regard to surveillance, compared to the reality, were irreconcilable with the mature understanding of what constitutes a liberal democracy. The paradigm shift, backed by legislation, towards full-scale surveillance in Europe, in other words, the retention of data, was rejected by the constitutional courts of five Members States of the European Union. At the present time, an application

made by two additional courts requesting a decision by the European Court in Luxembourg is pending and a decision is expected in the summer of 2014. One can only hope that the European Court will follow the rulings handed down by the judges at the constitutional courts and at the European Court of Human Rights in Strasbourg and declare the mass storage of data for no particular reason to be contrary to EU law. The approval by the Attorney General in December 2013 is therefore a good omen, in that he rejected the Directive on the retention of data. This would also serve to clarify the fact that the surveillance measures undertaken by the NSA, GCHQ etc. cannot be reconciled with the principles of European democracy. Data retention and automatic screening without reason are intolerable and are unworthy of a democratic state. They are detrimental to democracy, in that anyone who continually lives in fear of being observed by powerful authorities or companies, will soon adapt his or her behaviour. Any behaviour perceived to be unusual or that does not comply with the standard may potentially give rise to serious consequences, if indices, or even evidence, can be constructed from the dust generated by our day-to-day activities.

Even if at the end of the day, a single advantage for investigators can be found in programmes of mass surveillance in all spheres of life, do we really want to see ourselves turned into entirely transparent individuals? Is it desirable that a light be shone into every single corner of our lives? This is a question that is becom-

ing an increasingly contentious issue as a result of the current debate. The same also applies to the issue regarding the continually expanding collections of data being collected by privately-owned companies, which, as a result of each additional advance, are also opening up further surveillance capabilities for the authorities of State. As long ago as 1983, the German Constitutional Court handed down a wise judgment, stating that the informational self-determination is not only being jeopardised by State authorities, but is being placed under threat every single time our data are processed. That is why it is appropriate to apply the data protection regulations, especially to companies such as Google, Facebook, Yahoo! and Skype, whenever there are calls to do so as a result of the discussion concerning the surveillance activities being carried out by the secret services. After all, the NSA agents are not the ones who are filching data from inside our trouser pockets or who gain access to our bedrooms in order to collect data relating to our everyday lives. It is in fact those handy little devices produced by IT companies, which make use of programs, apps and services in order to gather, store and redistribute a wealth of data about us. Whether all of these are necessary at all or whether we could make use of anonymous services and much more secure programs that fulfil much more stringent data protection regulations is a topic that was something of a taboo in years gone by. One of the reasons for this lay in the fact that companies were able to do lots of nice things with our data, thereby generating a

great deal of money and market dominance for themselves. Ultimately, however, it must continue to be up to the individuals, as to what information they wish to reveal and what risks he or she wishes to incur when divulging information of a personal nature. It must not be the case that companies, and we ourselves, should become the private employees of the State authorities. That would constitute a surveillance society, in which distrust and despotism would reign supreme.

Instead of concerning ourselves with airing futile demands for total surveillance, it would be more appropriate to unify the standards governing democracy and fundamental rights that apply at European level, to such a degree that the police and the judicial authorities are actually able to meet the global challenges that exist, without scoring badly with regard to data protection. In addition, it would be appropriate to ensure that data protection in Europe is transformed into a market advantage for companies and consumers, in view of the fact that the many items of information will only be accessed, if there is a justified suspicion or specific looming threat. It would be appropriate to put a stop to the transfer of data to third countries, as long as no statutory protection has been implemented within European law in order to prevent EU citizens from being subjected to excessive and disproportionate measures. In a European democracy, it would be appropriate to ensure in an unambiguous way that laws that have been jointly agreed and the undertakings entered into regarding fundamental values and funda-

mental rights are transposed to an equal degree and are protected in all EU Member States. And it would be appropriate, finally to realise that a liberal democracy imposes limits upon the State. Not everything that is technically possible and not everything that can theoretically be achieved is actually desirable within our society.

One example of the removal of boundaries within surveillance measures is the proposal by the European Commission to collect the details of passengers travelling on flights in the European Union. Included in the *Passenger Name Records (PNR)* are the name of the passenger, the times of travel and routes involved, his or her contact details, the travel agency through which the booking was made, the method of payment, even the seat number in the aircraft and precise details of his or her registered hold baggage. All of these items of information are analysed automatically in real time. The declared aim of the draft Directive submitted in February 2011 was to detect terrorists and drug smugglers. A large number of Members of the European Parliament, however, regard the surveillance of passenger data to be a clear breach of the constitutional case-law of the European Union in relation to data protection and therefore regard it as a threat to central democratic principles. In the meantime, the PNR debate has developed into a hard-edged political argument between the Commission and a majority of the Council of Ministers on the one hand and the European Parliament on the other. Individual states, such as the United Kingdom

and Spain, even want to proceed one step further than was envisaged by the European Commission. They are demanding that PNR data be collected for passengers taking flights inside Europe itself. In mid-April 2012, a majority of those attending the meeting of EU Interior Ministers in Luxembourg spoke in favour of this proposal. Those who were against the proposal were Germany, Austria, Luxembourg, Malta and Slovenia. The European Parliament is probably now the only body that is capable of preventing the implementation of a screening programme covering the entire airspace of Europe.

Using the United States as an example, we can see what effects the proposed European surveillance scheme would have upon the lives and fundamental rights of us all as individuals. In the USA, the surveillance of passenger data was introduced more than ten years ago. Since the attacks on 11 September 2001, it has actually formed the core of the anti-terrorist measures implemented in that country. Under the strictest secrecy in a defence centre operated by the US Department of Homeland Security in the state of Virginia, the details of every single one of the 30 million passengers entering or departing the USA are analysed and linked to other investigative data. These include extended booking details provided by travel agencies and airline companies, such as credit card details, mobile telephone number, the IP address from which the booking was made and details of hotel and car hire reservations. All of this information is fed into detailed

hazard analyses, which are carried out using secret algorithms and subsequently evaluated.

As a result of the far-reaching powers of the US Ministry of Homeland Security, travellers are mostly completely uncertain about which sets of data have been associated with one another and what additional surveillance measures have been ordered on that basis. There have been countless examples that demonstrate that simply having an unusual name or making an unusual choice of in-flight meal can appear suspicious – in the worst case scenario, the indications can even lead to a permanent ban on entering the country. Most important of all, however, is the fact that the persons affected are unable to do anything if the investigators come to the wrong conclusion, as they are not permitted to see the data that have been gathered, let alone correct them or have them deleted. European travellers in particular are subjected to this type of surveillance – in the beginning, there was not even any basis in law that permitted the processing of personal details pertaining to citizens of the EU. It was not until the European Parliament had exerted pressure that negotiations got underway between the USA and the EU. In a number of resolutions, the Parliament had been highly critical of the approach adopted by the United States, as a result of which it also successfully initiated proceedings against the agreements initially adopted by the Council of Ministers. Following the entry into force of the Treaty of Lisbon, which grants the European Parliament considerable additional powers of co-

determination, an agreement regarding the transfer of the PNR data to the US authorities had to be renegotiated. Multiple drafts were rejected by the Members of the European Parliament and only following intensive renegotiations with the United States could a majority decide in favour of an agreement that governs the transfer of data to this day. Most recently, Washington had even threatened to withdraw permission for aircraft belonging to European airlines to land.

For those in favour of expanding the surveillance measures in Europe, the adoption of the agreement provided an opportunity to make the evaluation of the PNR data acceptable, even in Europe. Whereas the liberal EU Commissioner Cecilia Malmström argued only a few years ago against the mass evaluation of passenger data by the US authorities, she has now gone as far as to submit a proposal for a European passenger data analysis programme which is not in any way inferior to the surveillance system used in the US. At the same time, Malmström is quick to play down the scale of what is being proposed and, ironically, is promoting it as if it were a Data Protection Act. The Commissioner's intention is clear: her aim is to do everything possible to avoid creating an impression that the retention of data is being used for the purpose of screening, or even profiling, in the course of which different items of information are merged together in order to form profiles that are thought to be those of an »agitator«. But that is exactly what is alleged to be taking place.

And it is not only members of the European Parliament who are expressing criticism about the surveillance of all air travellers. Officials within the European Commission and in the legal department of the Council had already realised that the planned Directive could not be reconciled with the opinions of the highest courts in Strasbourg, Luxembourg and Karlsruhe. As yet, the supporters of the proposal have still not provided the evidence required by the European Court to confirm that any form of surveillance is »necessary and proportionate within a democratic society«. Even in reports designated as Top Secret, the only evidence offered to confirm the necessity of introducing passenger surveillance consists solely of individual cases, without however explaining the circumstances of the investigations in each case or the role played by the passenger data themselves.

Up to the present time, no decision regarding the evaluation of European passenger data has yet been made. At the same time, the issue no longer relates solely to the surveillance of air travel: even now, the Italian government is requesting that the gathering of data be extended to include all ferry routes inside Europe. And it will only be a matter of time before authorities start to demand that all train travel in Europe be subjected to surveillance in the same way. In short: there is a possibility that every journey undertaken by the roughly 500 million EU citizens – in the air, by sea and on land – will be recorded and analysed. If the European Commission and the Council have their

way, they would not only have successfully copied the surveillance practices adopted in the USA, but would potentially have expanded their scope by some considerable margin. One can only hope that the European Parliament puts a stop to the first stages of these practices and does so quickly and decisively.

But the trend, however, is rather different. A majority of a large coalition in the European Parliament wants to make mandatory the installation of eCall systems in all vehicles, without the ability of the owners or drivers to switch them off. This would create a situation in which all passenger cars and heavy goods vehicles would be fitted with a mobile phone device incorporating a SIM card, or a GPS transmitter, the position of which could be determined at any time by the mobile network operator. The actual idea behind this is to locate a vehicle in the event of an accident, thereby enabling injured persons to be rescued more quickly. The consequences of the ability to locate any vehicle are being completely swept under table, however, especially seeing as it became clear during the initial debates that the public prosecution and security services should also be allowed to access this type of data, which is something that is already ever-present. No database or system is safe from the attentions of the state investigative authorities: during the past few years, legislators have simply diverted a great many private-sector and state-run data processing systems from their intended purpose, in order to use them to pursue the security interests of the State. In the case of

the retention of data and the analysis of air passenger data, laws are even being discussed and adopted that actually require such data to be retained. The next area in line is the data from toll systems and the ticketing data used on our railways and by local public transport systems. The recording of personal details is becoming increasingly prevalent in all forms of travel, even down to individual travel. And this also extends to the collection of personal data. There is nothing to prevent the in-car journey recorder, which was mentioned earlier in this book and keeps a detailed record of our driving behaviour in order to pass this to our insurer, from being accessed by the authorities in the very near future. If not earlier, this will occur whenever a serious, but undiscovered and unpunished criminal act occurs, which, at a time of collective shock, can be used as a reason to expand state access to private-sector data.

The debate regarding the preventative profiling and analysis of all travel data (known as metadata) formed only the tip of the iceberg that clearly came to our attention in summer 2013, if not before. The system that is used in order to collect and profile all types of seemingly unimportant bits of information – however technical and lacking in content those items of information are alleged to be – has secretly been undergoing further development within the security services. With the help of computer experts it has bought in, the NSA and its partners have developed programs in the Western democracies that will soon be capable of carrying

out a full analysis of the flow of data and to search it for correlations and unusual features. Commencing with the ability to search for keywords within internet-based communication through to searches for an unusual tone or aggressive form of expression, the range of tools available to the secret services is nowadays almost unlimited. As too is the mass of information sources available, as was demonstrated by the smartphone game »Angry Birds«. The game collected data for no particular purpose; however these data were evaluated by the NSA and by GCHQ.

The documents made public by Edward Snowden show that, fundamentally speaking, total control knows no limits, once we have taken that first step towards digitisation. They also demonstrate that in the case of the measures already implemented, it is simply a case of implementing a system that is an end in itself and will involve creating a crystal ball that operates as accurately as possible and will enable investigators to predict the future and, by carrying out checks, to prevent certain events from occurring. Driven by the delusion that they must not let anything go unnoticed, they are actually losing sight of the true tasks of the security authorities, as well as of the principles underlying a democratic and liberal society. Privacy and individual self-determination are simply regarded as a danger, whilst their actual task is that of mass surveillance. The failure of politicians to recognise this negative development and to correct it, is significant. The verification bodies operated by parliaments, which meet in secret, are be-

coming part of the secret-service approach, are limiting their verification capabilities – as are the governments themselves – to the objective of maintaining more effective secrecy, in the interests of national security. As a leading Member of Parliament in the investigation conducted by the European Parliament into the mass surveillance carried out by the secret services (which will be concluded in spring 2014), I came across colleagues from national parliaments with responsibility for controlling the secret services, who, even a number of months after Snowden's revelations, knew less about the programmes being conducted by their country's secret service, than we ourselves were able to find out during our brief investigation. Instead of considering the effectiveness of the measures, the principle that national security is sacrosanct has become a mantra.

Even the political reactions that emerged in the immediate aftermath of the devastating attacks in Norway in the summer of 2011 revealed the lack of knowledge and the inability of politics, when it is a matter of a state being capable of addressing the challenges posed by a globalised and digitized society. The symbolic responses that were forthcoming comprised the retention of data, without grounds, relating to all forms of telecommunication, the blocking of websites containing illegal or dangerous content and the reduction of the possibilities to operate anonymously within the world wide web. The political right wing gives the impression that these three measures are capable of preventing the

radicalisation of individuals and the escalation of the types of violent acts undertaken. The fact that quite a number of years ago, this particular theory was found to be incorrect, clearly plays no part in the thinking of the particular politicians involved, and this is to the detriment of freedom and security in Europe. Instead of addressing the true causes of the current problems, the priorities being set in the areas of domestic and security policy are completely wrong. Nor are they addressing the massive erosion in the powers of a state to impose rules and regulations, which can certainly not be prevented in the form of national laws governing the world wide web.

The types of action required are also just as contentious as they are incapable of bringing about a solution to the problem. They form a populist selection of measures taken from the toolbox of a police state. In that regard, globalisation and digitisation are posing new challenges in terms of internal security and the work of the police and those challenges now require more complex solutions. It doesn't actually matter how many security agencies and surveillance measures are adopted at EU level. If some of the police stations that are present on the ground are not even adequately equipped with good internet connections or IT forensics facilities, the rate of resolution of internet-related crimes will not improve. The internet is not a new world, but is simply an extension of the existing one, which requires cross-border rules and regulations, but does not require politicians to reinvent the wheel. And

if the resources for police patrols continue to undergo financial cuts, especially in rural areas, and federal and EU funding continues to be directed towards the combating of international terrorism in a manner that goes almost unquestioned, there can be no prospect of any reduction in the actual rates of crime. At European level in particular, we must finally seek to identify new approaches that will enable crime prevention to become more effective in the digital age and to identify and prevent criminal acts more quickly. Even in the analogue world, effective policing is capable of operating without comprehensive banning orders, number plates on our foreheads or comprehensive surveillance systems.

For many years now, Ministers of the Interior have pursued policies that will bring forth a rapid outcome and have pursued the wrong priorities. It is therefore no surprise that increasing numbers of people no longer regard their parties as the representatives of a system of meaningful politics or of internal security. They wish to see a society that is actually safe, as opposed to a surveillance state that provides a feeling of security. Instead of costly body scanners at airports or creating additional collections of data, it is a case of investing once again in measures that will genuinely combat crime. And instead of outsourcing tasks that are presumed to be those of the police to internet providers and censorship authorities, we need not less but more money and value to be placed upon the effort to combat ideas born of inhumanity and to design alter-

native and meaningful forms of culture, media and the exchange of information via the internet. In particular, this would include the more effective training of new police officers, ensuring that local police stations are adequately equipped and strengthening a vigilant and united civil society, in which anonymity does not give rise to suspicion, but should lower the threshold of participation. After the dreadful events that took place in Norway, absolute security is and will remain an illusion. Actually achieving a reduction in the rate of crime is however a tangible objective that will simply require the right political decisions to be made in Europe.

Police action is primarily legitimised by the fact that people see it and are able to value it. A Chief Inspector of police, who walks through a pedestrian area in the city centre and keeps a look-out, greets people and is seen to take action, will receive a high degree of credibility and recognition for the work that he does. Without having received authorisation by means of complex, democratic processes of opinion-forming, his actions and his monopoly of power will be afforded immediate legitimacy on the street. Transparency and openness are values that engender trust in the institutions of a democratic state. Of course, not all police actions that took place in the past could have been predicted or were seen by us all. In the broadest sense of the word, predictability was always an important pre-requisite in the case of actions undertaken by the state within a democratic system. Only in that way is it possible to grant legitimacy to the monopoly of power exerted by the state. A

society, which, without knowing anything about the actual steps involved, grants authorisation for an incursion into people's fundamental rights or even for the exercising of power, will be poorly equipped when it comes to organising effective control over the Executive. Predictability is one of the core characteristics of a democratic state. The measures taken in order to combat the terrorist activities in the 1970s and 1980s serve as an indication of the challenges that face the Federal Republic of Germany as a democratic state. Investigation methods such as dragnet controls and undercover investigators are creating a situation in which the decision-making process adopted by the security services is increasingly difficult to determine. This massive information gap between the State and its citizens is giving rise to a loss of control over the monopoly of power on the part of democratic institutions and of the public. With the new technologies offered by the digital domain and the almost invisible profiling of personal data relating to us all that takes place almost entirely out of sight, this loss of control looks like it is here to stay.

In this situation, many people have confidence in the fact that state institutions will behave in accordance with the law or will at least behave »well«. After all, they wouldn't pursue anyone who had not brought it upon themselves or been guilty of any crime. In their opinion, anyone who has nothing to hide, need not have any worries. Those people regard »having something to hide« as having committed an offence or acted unlawfully. The fact that collective surveillance that is

intended to uncover such acts also brings to light a considerably greater amount of information about us all than is relevant for the purposes of society, the security services or for the prosecution of crimes is something that very few people acknowledge. Depending upon the evaluation criteria employed, it can make a significant difference, whether an alleged suspect receives a regular income, is involved in a settled relationship or is behaving in a strange manner. The fact that all of this information need have absolutely nothing to do with a justified suspicion will not alter the fact that depending on the information available, this person will be viewed differently or will become the focus of investigative or compulsory measures. This takes the form of an apparent correlation that acts as a disfavour to the person concerned. The more information is available, the more likely it will be that everyone who behaves in a manner that does not conform to the norms of society will fall under suspicion. This especially affects those who can do nothing to prevent themselves from failing to conform to the norm. People with disabilities, minorities, the sick or people who are disadvantaged in some way find themselves in a difficult position, as they are frequently suspected of forming a hazard. But these are only the most obvious examples. Consider, for example, whether you would reveal everything to everyone, without hesitation. For example, would you reveal to your employer where you just spent the night or what you do in your free time? Or would you tell your health insurer? Would you really want to tell the

police that you regularly find yourself driving through a traffic light when it is on red? In the world of big-data analysis as a means of detecting crimes, this information would at least increase the likelihood that you would be prepared to break some other types of rules.

The film »Minority Report« actually takes the idea of an all-knowing police state to the absolute limit. Using what is known as a »Pre-Crime« system, it is possible to predict whether someone will commit a crime in the immediate future. In the film, this is achieved by means of the »pre-cogs«, who are capable of looking into the future and sensing who is likely to turn delinquent soon. An alarm then sounds and the »suspect« is then immediately arrested, brought before a court and sentenced for an act that he or she was going to commit in the future. In the world of big data, mundane items of information about our everyday lives are fed into massive computers. Millions of items of metadata about our movements, communications, purchases, contacts and so on are brought together by complex algorithms in order to form profiles, which are then compared to the profiles of dangerous individuals. These are drawn together from the mountains of data relating to the past and are used in order to calculate the likelihood that a criminal act will be committed. In this way, our behaviour, our personality, our environment, our entire lives are searched for possible aberrations or circumstances that could constitute a danger. At the end of the process, we are assigned a score, which pigeon-

holes us in the same way as would be done by a bank or insurance company. The only difference is that this is no longer a case of establishing someone's credit or insurance rating, but the likelihood that we are or may perhaps become suspects or criminals.

Finally, we need to ask the following question: What will happen, if one of those algorithms calculates that it is 80 % certain that I will commit a murder tomorrow? This would not be based upon any specific suspicious act, but purely upon a big data analysis of my everyday life. Would society still allow me to retain my liberty? You can surely imagine how long it would be, before a considerable number of people would demand that I be taken into preventative custody. To those people I say: You have something to hide! And I say that with justification, as no-one would be able to escape the arbitrary nature of a fraudulent or improper evaluation of their most intimate secrets and of their peculiarities. The only protection that is available to prevent this is a system of data protection law that is effective, coupled with a healthy discussion about the measure of mutual control that is appropriate within a liberal, democratic society. In the early 19th century, Jeremy Bentham developed a type of prison construction, in which solely the possibility of being observed maintained discipline amongst the inmates. Known as the »panopticon«, this took the form of a round building, in the middle of which was a tower, from which a prison guard could observe all of the prisoners. Their cells, which opened onto the tower, were pointing towards the tower, but did not allow anyone to see inside it, which meant that the pris-

oners could never know, whether they were actually being watched or not. The one thing that they knew for certain was that they could be watched, whatever the situation. And that fact alone ensured that complete discipline was maintained amongst the prisoners. This was an architectural manifestation of an effective surveillance society. In the 20th century, the philosopher, Michel Foucault, developed Panopticism, in which such institutions were to be used for the purpose of disciplining society. Anyone who recognises that type of society as a dystopia, such as the one portrayed by George Orwell in his book »1984« or by the German author Juli Zeh, in her book entitled »Corpus Delicti«, will quickly understand that the retention of data and the mass surveillance programs of today form the pillars of a panoptical, discipline-based society, in which we no longer need to be sanctioned for deviant behaviour, as we are already imposing sanctions on ourselves, by obediently adapting our behaviour in advance, out of fear of the sword of Damocles that is hanging above our heads, in the form of the constantly threatening surveillance and imposition of sanctions by the State and by society. Even today, anyone who is curious to know what an atom bomb is made of or to find out the details behind the murder of a politician will certainly consider what will happen, if the algorithms identify that search as dangerous and I suddenly come into the sights of some state power? And what if I am arrested one day? Is it worth all that? Anyone who does not wish to ask himself these questions, but wishes to preserve the valuable commodity of free thinking people, will have no alternative but to fight to maintain our rights of data protection.

The political and industrial complex

The quick and simple solution adopted by politicians in response to security threats more frequently involves announcing new, more promising surveillance measures. In this era of global and abstract threat scenarios, the all-knowing state is being stylised as the redeemer. At the same time, private-sector companies that are constantly presenting new, more far-reaching data processing and surveillance technologies are the ones that will profit from this solution. This results in an identical interest in an increasing need for security. Security politicians and the manufacturers of surveillance technology are painting a picture of new levels of threat and are making sure that they are able to herald the advent of a new level of control.

I first became aware of the extent of this development when, as a newly-elected Member of the European Parliament, I was invited to attend the European Police Congress in Berlin in February 2010. In the foyer of this extremely costly meeting between police and politicians, there was an exhibition highlighting the latest developments in surveillance and repression technology. In the event hall, a manufacturer gave an advertising presentation for smart, drone-supported video surveillance systems. Whereas in the past century, it was the weapons industry that was in cahoots with politicians around the world, the surveillance industry has taken on that role in the 21st century. Conflicts are also more frequently being played out via IT systems. Since the

millennium, discussions have been taking place about the resources that could be deployed in the event of a cyber war, not that any disputes have as yet been settled by means of cyber weaponry. The export of IT systems for the surveillance of smartphones and computers and the infrastructure required in order to carry out censorship and blockades is becoming an increasingly important factor within the economy, as increasing numbers of states and private players are expanding their equipment base. No effective control is taking place, however, in order to ensure their correct use, nor are the consequences of such exports being checked, especially in the case of exports to states with repressive regimes. On the contrary. Research initiatives financed by democratic states or private-sector service-providers develop penetration tools that enable data to be called up from IT systems or that install back doors in devices and programs. At the same time, the very same technologies end up again and again in the hands of unsavoury parties, such as the dictators in states with repressive regimes or organised criminal gangs. Again and again, we are witnessing a dangerous double standard, in which criminals and repressive regimes on the one hand are being sentenced after having broken into the systems of companies or private individuals, whilst democratic states and major IT companies themselves regard those very same practices as legitimate.

This became clear when it became known that the NSA and its cooperation partners in other countries had themselves financed and programmed systems

and programs for that very purpose, as a means of breaking into the protected communications systems of telecommunications companies or into the smartphones of private individuals. In order to achieve this, the organisations appointed hackers and installed supercomputers, which, in individual cases, overrode the privacy and property of third parties by surmounting any type of security feature or by setting up carefully conceived back doors. Without effective parliamentary control, or with the acquiescence of the very institutions tasked with controlling such matters, the secret service agencies concerned were acting in a manner that lies beyond what can be described as being in accordance with the rule of law. By providing massive financial resources to its cooperating companies and due to the interest of all concerned in the evaluation of the data, a political/industrial complex was able to be developed that created, at the expense of the freedom and fundamental rights of the people in all countries, an increasingly comprehensive system of surveillance, to the detriment of the community, which could not, or did not wish, to know about it. It was only the courage of people such as Edward Snowden that brought the existence of this complex to light bit by bit and placed it before the democratic public for debate.

Wherever state power protects its own interests, what we see is a massive accumulation of secrecy that makes it increasingly difficult for those in power to bring to bear any control. Whilst repressive regimes are subject to almost no limitations or controls, at-

tempts are being made in constitutional democracies to ensure that any accommodation of these is kept as small as possible. The linchpin of these attempts to limit constitutional democracy in Western states is the concept of »national security«. Both in the USA as well as in the Member States of the EU, national security is all but exempt from public and constitutional control. Only the parliamentary control bodies operating in secret and courts sitting in secret are able to receive a glimpse into the modus operandi of state power in these areas. The intelligence services in particular are especially effective at ensuring that their information is does not come to the attention of such controlling bodies. As was demonstrated in the late 1990s by the »Echelon« affair and later, in 2013, in the case of the Snowden documents, a massive monopoly of intelligence plays a key role in that regard. The highest level of surveillance goes hand in hand with the greatest possible secrecy. What is particularly problematic about this is the fact that since the advent of the large IT companies such as Google, the secret services have found some powerful allies that share the same interest in developing a monopoly of knowledge. Together, the resources they have at their disposal in order to push ahead with the further upscaling of surveillance activities and the ongoing drive to acquire knowledge on the one hand and to ensure more effective secrecy on the other, are almost infinite.

The greater the gap between the democratic public on the one hand and the political/industrial complex on the other, the further the fundamental principles

underlying the constitution will be eroded. Principles such as »No intervention without legislation«, jurisdiction by the type of court designated by law and a fair hearing are becoming increasingly less significant, the more relevant the exceptions become. Whereas in the 20th century, national security was restricted to the monitoring and pursuit of agents working for other powers and was primarily directed towards crisis zones and war zones, national security witnessed a tremendous expansion on both sides of the Atlantic in the aftermath of 11 September 2001. Nowadays, the security and criminal prosecution authorities are much more active in the national security domain. A broad definition of the term »terrorism« (in its annual report, Europol, the European police authority, actually coined the term »animal rights terrorism«), the inclusion of criminal acts that occur across national borders (bicycle thefts in border areas are already included in this category) or of the use of the internet as a means of committing a criminal act (the infringement of intellectual property rights is often referred to in this regard) and of cases involving serious international crime and newly-emerging asymmetrical threat scenarios are leading to circumstances in which in many everyday situations within constitutional democracies, the rules applicable to a state of emergency now apply, under which the fundamental rights of us all have only limited validity and the possibilities for state surveillance have been expanded. In fewer and fewer cases are the conventional control bodies that date back to the pe-

riod of the Cold War able to maintain an overview over all of these measures, let alone demand that the most fundamental limits are adhered to.

As a result, the political/industrial complex is creating for itself a special right that is edging dangerously close to those enjoyed by the repressive regimes in non-democratic states. The precise manner in which it is managing to bring together the capitalist market economy with a state surveillance structure is extremely similar to the actions of states such as China or Russia, especially in view of the fact that it is only inside the country itself that any confrontation with the vague boundaries of state power takes place. As soon as the escalation of security technology takes place at the outer limits of the state or even beyond the twelve-mile zone, the thin veneers of an allegedly democratic constitutional state begin to fall: for years now, the European Union has been reinforcing itself to turn itself into Fortress Europe, which, as a result of programmes such as Eurosur, the Schengen and Eurodac information systems and the border protection agency, Frontex, is able to keep immigrants who are presumed to be illegal out of its territory and is able to monitor, imprison or place them in life-threatening situations, while disregarding their fundamental human rights. And it is precisely this that enables any countries with repressive regimes to reject any admonishment from the West about their approach towards human rights. All of this goes hand in hand with the development and financing of security technology, such as drones,

smart cameras, Trojans and satellites. An escalation is underway that is increasingly looking like a military operation. Technology that was previously used predominantly in the external and security policy between states and in war-like conflicts is nowadays used more frequently in internal political confrontations between the state and its citizens. One of the particularly alarming aspects of this is the fact that the carefully drafted and democratically approved rules of a liberal democracy are giving way to the principles and values of a system of public international law that has been developed between nations. The best example and a pioneer of this development is the counter-terrorism lists operated by the UN Security Council, which solely contains the names of those suspected of having committed terrorist acts and requires all states to deprive those individuals of all of their rights. The individuals concerned are no longer afforded any legal protection before a national court, nor are their fundamental rights protected, even if someone has ended up on a list of that type simply as a result of being confused with another person. The national security of states and the external and security dimension dominate discussions. Surveillance measures and data collections in those areas do not abide by any conventional rules and are therefore also not subject to the rules of data protection. It is no coincidence that for many years, states have been vehemently refusing to agree binding joint standards for the exchange of information. Even the Member States of the EU have only agreed a set of extremely imprecise

framework conditions governing mutual assistance in police and judicial matters, from which governments are able to cherry pick the parts they wish to adhere to. National security and defence are actually excluded from the effects of EU law in their entirety. EU Member States are not bound to abide by any type of joint rules in the case of data collected by the intelligence services and the military – not even by the binding EU Charter of Fundamental Rights. This shows how urgent it is to bring back the democratic debate about the application of fundamental standards governing security measures. But the political/industrial complex has Europe firmly in its grip. Every critical voice is branded as dangerous. When, in February 2010, I argued in favour of a refusal to allow the USA to analyse banking data, I was reproached by high officials from the EU and the USA, stating that I was therefore willing to accept that there would be hundreds if not thousands of potential additional victims of terrorist attacks. This is a logic that is not an isolated case. When body scanners were introduced (which, at a purchase price of around half a million euros a piece, exceed any test of proportionality); when the retention of data was introduced (which imposed costs to the commercial sector and therefore to consumers amounting to billions); on the acquisition of intelligent drones and satellite systems (developed using funding provided from EU research subsidies); or in the case of the use of flight, toll or banking data (which, in fact, constitutes a privatisation of the state security apparatus): in all of these

cases, the state and the security industry are working together to bring about the technological escalation of our surveillance society. The parade themselves before us with their fear-mongering and earn good money by doing so. In many cases, this involves a not inconsiderable combination of politics and industry. The »Kangaroo Group« within the European Parliament, which regularly brings together MEPs with important players within the security lobby, forms just one example of this. Members of the Kangaroo Group including influential MEPs, especially those from the Industry and External Trade Committee, together with lobby representatives from the industry meet to enjoy an exquisite three-course menu in the Members' restaurant of the European Parliament in Strasbourg and swear to uphold the necessities of their shared concerns. The direct benefits for the Members themselves and for the Ministers can only be documented in rare cases. What is clear, however, is the fact that the lobby acting on behalf of large-scale companies has many methods that enable it to exert a considerable influence with regard to the regulatory guidelines and economic policy priorities in Brussels. In that regard, the security industry and large, data-hungry IT companies are often singing from the same hymn sheet. They have the feeling that they are not being observed, as do a great many MEPs and ministerial representatives. In order to change this, what will be needed is a massive deployment of those who wish to bring transparency into politics. Examples of this include initiatives emanating from within the

realm of civil society, such as Statewatch.org or LobbyPlag.eu. But what is also needed is a lively and audible public that closely scrutinises governments and parliaments – especially in matters relating to EU decisions. It is clear that the fundamental right to data protection in particular is something that people need to fight for again and again., as politics and the business sector often have a shared interest in weakening our information self-determination.

A plea to politicians and to society

Fundamentally speaking, it is a matter of historical good luck that in the midst of what has been the hardest debate to uphold the self-determination of individuals, the severity with which all of our lives are already affected by continual control is finally becoming clear. The courageous step taken by Edward Snowden to publicise the data-collection practices conducted by the secret services of Western democracies and the collaboration taking place between information-hungry internet companies and state security services has kicked off a long overdue debate within society regarding the limits of democracy and self-determination on the one hand, and of automation and calculation on the other. The liberal constitutional democracies of the West in particular are suddenly being faced with the question as to whether the fundamental principles of our society still exist in reality. We are currently witnessing a sea-change, the scale of which is not dissimilar to that of the Industrial Revolution. Whilst the response to the technical and commercial upheaval that took place involved the creation of social standards and standards regarding working conditions, such as the foundation of trade unions, what is needed in an era of digital revolution are standards governing areas such as data protection and consumer protection, as well as new forms of control with regard to the freedoms and rights of individual citizens. Politics bears considerable responsibility for ensuring that such standards are put

in place. Politicians must take the findings that have been established so far and use them to create a foundation, which, amidst the current upheaval, is suitable to provide an effective framework that will enable us to co-exist. At the time of writing, however, they are not doing so. Many states, their politicians and their citizens are steadfastly holding on to perceptions that originated in the analogue era, as well as to their structures that are dominated by nation states. Only a few forward-looking thinkers are currently aware of the fact that law and social values are becoming eroded as a result and that every moment we continue to hesitate represents a loss of sovereignty.

Digitisation is casting our society into a situation of turmoil that is similar in scale to that of the Industrial Revolution. What is needed, therefore, is an equally intensive discussion about the rights and freedoms of citizens in the digitised world, just like the one that took place in response to the industrialised world. Informational self-determination forms a fundamental aspect of an active citizenry. The sovereignty of individuals when it comes to their ability to make decisions regarding the use being made of their own data forms a pre-requisite for a balance of power between individuals and the powerful players within the State and the economy, the control of whom is becoming increasingly imponderable.

The threat posed by data protection serves as an example: for years now, the major internet companies in Silicon Valley have been circumventing their

data protection obligations and are generating substantial profits as a result, especially in Germany. Only in extremely rare cases are any court judgments handed down and tangible sanctions are hardly imposed at all. As a result of large-scale lobbying activity, the internet giants are able to block any form of regulation in the USA or the EU. In the US Congress, they have successfully blocked any attempt to establish compulsory data protection laws applicable to the private sector for a number of years now. In Brussels and Strasbourg, the US Chamber of Commerce, which is the most powerful commercial representative body in the world, is pulling no punches and is availing itself of the cheapest forms of populism in an attempt to counter the attempts by the European Commission to improve the current data protection rules that apply in Europe. It is stoking fears of massive costs to be borne by companies, is warning that growth will stall and is speaking of a loss of prosperity of around three billion – per year, that is – , if data protection remains as it has been in Germany for years. These are the findings of a study that the Chamber happened to present at a number of large-scale events immediately prior to crucial negotiations in the European Parliament regarding the EU Data Protection Regulation in a large number of capital cities of EU Member States, in order to warn politicians about the new data protection regulations being planned.

In view of the revelations of large-scale surveillance by the US secret service, the question once again arises regarding the implementation of data protection,

informational self-determination and privacy in the digital era. The answer to this can only take the form of a strong Data Protection Regulation issued by the EU. Overall, however, those who wish to uphold civil rights, constitutional rule of law and democracy still find themselves in a minority. In that regard, data protection nowadays forms an express part of the binding EU Charter of Fundamental Rights and the European Human Rights Convention of the Council of Europe. Also included are the postal and telecommunications confidentiality, the fundamental right guaranteeing the confidentiality and integrity of IT-based systems and on a very general level the freedom from arbitrary incursions by the state authorities. All of these are fundamental principles underpinning a constitutional democracy in the form that we and our forebears fought to achieve it in the aftermath of dictatorships, reigns of terror and wars in Europe. Data protection forms a fundamental part of any democracy. The surveillance scandals of 2013 triggered a debate about the handling of fundamental and human rights in a digitised and global world, which was long overdue. Nowadays, it is also clear that the USA is not the only country to have exceeded the limits on a major scale. The secret service of the United Kingdom and those of the other EU Member States have also taken actions that have undermined the foundations of constitutional democracy. It appears that a feeling for these values has been completely lost, not only with our transatlantic partners in the United States of America, but also here, in

the very heart of Europe. The massive extent to which various parties have clearly acted in contravention of fundamental constitutional provisions, the provisions of conventions and treaties and the judgments issued by the very highest courts, and have been doing so for many years, is incomprehensible. As recently as March 2010, the Federal Constitutional Court of Germany rejected the storage for six months of all communications framework data in the context of the German Retention of Data Act, finding it unconstitutional. In the case of S. and Marper versus the United Kingdom, even the European Court of Human Rights in Strasbourg imposed clear boundaries to be applied to non-specific surveillance. Investigative activity without a specific objective is therefore incompatible with the protection of human rights. The judges are most likely to follow the opinion of the Advocate General of the European Court, who stated that the EU Directive on the Retention of Data contravenes EU law. And yet the European Commission and the Ministries of the Interior within the EU Member States are continuing their work to develop large-scale surveillance programmes. Under the heading of combating terrorism and almost unseen by their political leaders and beyond the view of public control, a policy has been pursued for over ten years now that places individuals as a whole under suspicion and is based upon the principle that they almost want to be able to read from our faces, whether we pose a danger to security. If the number of voices in the political domain that state that the mass sur-

veillance of communications processes carried out by secret services is disproportionate, increases, this will be a positive sign in favour of democracy and the constitutional rule of law. It would however be extremely necessary to put in place clear boundaries in the form of legislation and for them to be checked in practice. Since the emergence of the NSA scandal, no investigative or data protection authority in Europe has felt it necessary to launch an investigation into the attack by secret service agencies upon servers and systems belonging to telecommunications companies, such as Belgacom in Belgium. This makes it clear that such attacks are not in keeping with the national security of the states concerned and cannot be legitimised by means of any treaty. Both criminal law and data protection law would be of relevance in this regard and ought to be enforced in a clear and unambiguous manner.

But particularly whenever they consider the enforcement of those boundaries, many of our current politicians are clueless, as they are aware that over a number of years, they surrendered control to global IT companies or secret services acting on their own agenda, which themselves are now imposing their rules in accordance with their own interests and standards. The paramount task now facing sovereign Members of the European Parliament is to dedicate themselves to actively protecting democratic principles relating to the fundamental and human rights of their citizens. The data protection reforms in the European Union provide an ideal starting point from which to realise this.

What is needed is, again, what the German Constitutional Court in 1983 defined as control by individuals over their personal data: the possibility to ensure that each and every individual retains their informational self-determination, as an expression of their dignity and of their rights as an individual. Data protection means the protection of human beings! Whoever it is that processes our data, is of no significance. What matters is whether we wish to make our data available at all and subject to what conditions. It is time for us all finally to show our true colours!

Acknowledgements

This book has been written in an era in which, every day, new revelations on intelligence agencies' mass surveillance come to light because of the brave act of whistleblowing by Edward Snowden. The English translation is published a year later than the German original yet the issue of privacy and the protection of personal data in a digitalized society is as pressing and pertinent as ever. I am happy to contribute to this debate and hope (and know) that there will be still many more outspoken contributions. The future of digital self-determination is one of the biggest challenges of our time and I will be continuing to work on this issue and to keep it high on the agenda of the European Parliament – the most important decision making body for the lives of European citizens. But of course this issue affects everyone around the globe. I receive many letters and e-mails which call on me as rapporteur of the EU's planned data protection regulation to safeguard their fundamental rights in a global digital society. People pin their hopes on the European Union to set high standards for the global market. Their demands are backed by huge consumer and civil rights groups, especially from America and Europe, who press the European Parliament to take action since their own Parliaments and Governments appear incapable of delivering the solutions needed to protect citizens and consumers today.

I would like to thank the publisher Drömer/Knaur for their help in writing this book as well as for allowing me to translate and print this book in English at my own cost supported by the European Parliament. I welcome any questions, remarks or critiques on this book as well as in relation to my work more generally as a Member of the European Parliament, where, since 2014, I have served as a Vice-Chair of the Civil Liberties, Justice and Home Affairs Committee. Contact details and further information on the issue of data protection and privacy, as well as on my work on civil liberties in the digital age, can be found on my website *www.janalbrecht.eu* (mostly in German, parts in English) or on *www.greens-efa.eu* (English available).

The big battle on freedom in a digital age

It is being pulled out of our pockets unnoticed: the most personal information about ourselves. With the virtually unlimited possibilities of data processing, we are not only becoming »transparent citizens« – we are also being exploited and disenfranchised. EU data protection expert Jan Philipp Albrecht sheds light on the current drawbacks of data protection, what politics needs to do about it and how we can protect ourselves.

www.janalbrecht.eu

ISBN 978-3-00-051137-0