**Purpose or Interest: that is the question!**

**Prof. Lokke Moerel & Prof. Corien Prins**

|  |
| --- |
| “We cannot simply start by asking ourselves whether privacy violations are intuitively horrible or nightmarish. The job is harder than that. We have to identify the fundamental values that are at stake in the issue of ‘privacy’ as it is understood in a given society. The task is not to realize the true universal values of “privacy” in every society. The law puts more limits on us than that: The law will not work *as law* unless it seems to people to embody the basic commitments of their society.”James Q. Whitman, The Two Western Cultures of Privacy: Dignity versus Liberty”, *The Yale Law School Journal*, 2004, p. 1220. |

Let us imagine a mobile phone application that traces your movements and phone calls in order to inform you whether you are likely to catch influenza. The app can even tell you which friends you should avoid in order to minimize your risk of catching the flu - even if those friends have not yet been affected by it themselves (this is not fiction, see research MIT of Professor Pentland). Would you install this application on your smartphone as soon as you had the chance? Then imagine the use of a similar app by the World Health Organization (**WHO**), in order to protect public health in cases of pandemics. Two applications that both collect and process personal data for the same purpose: the monitoring and personalized prediction of health and illness. But the sentiments that these two applications give rise to are likely very different.

When we pause to reflect on this, the conclusion is that it is not so much the **purposes** for which personal data might be used that is the primary consideration here, but rather the **interests** that are served by the use of the data collected. And yet, both the current and the upcoming EU data protection regime are based primarily on the **purpose** for which data are collected and processed, while the **interests** served play a much more subordinate role. This raises the question of whether this legal regime can be effective and can be considered legitimate as we move into a future whereby society is driven by data.

In short, we believe that a test which is based on whether there is a legitimate interest for data collection and its processing (and possible further processing) will provide for a more effective data protection regime that will have more legitimacy than the assessment under the existing legal regime that is primarily based on the **purpose** for which personal data are collected, which requires that : **a.** data may only be collected and processed for certain legitimate purposes (*purpose specification*), and **b.** data may not be processed further if this is incompatible with those purposes (*compatible use*). The *data minimization* requirement is also related to the purpose: no more data may be processed than is necessary for the relevant purpose. Due to social trends and technological developments (such as *'big data'* and the *'Internet of Things*’) the time has come to abandon the principle of purpose limitation as a separate criterion and recognize the legitimate interest principle as the principal (and only) test for all the various phases of the life cycle of personal data: collection, use, further use and destruction. This proposal also means, therefore, that the other legal grounds for the processing of personal data (such as consent and the performance of an agreement would no longer be applicable as independent legal grounds. In our proposal these other grounds and principles remain relevant, but then as part of the legitimate interest test. For example, the principle of data minimization would continue to be relevant. This principle is already now part of the legitimate interest test via the principle of proportionality. Data minimization means that no more data may be collected and processed than are necessary for the relevant legitimate interest. The same applies to the grounds of consent and performance of a contract. In our proposal, these will be a factor in evaluating whether there is a legitimate interest. Merely asking for consent is not sufficient, but consent (*opt-in* or *opt-out*) could be the final element in determining whether the legitimate interest test has been met. The existence of a contractual relationship will also be one of the factors that play a role in the assessment whether there is a legitimate interest. Relevant factors are: the status of the individual (is he/she an employee or a customer?), the status of the controller (e.g., is it a company with a dominant position in the market or does it concern an employer in its relationship with its employee?), and the implications for that individual (which may be greater in the case of contractual dependency). It may well be that the more specific the contractual relationship is, the more restrictions there would be on the use of the data. This represents a departure from the current situation, under which clicking ‘OK’ for contractual terms is the easy way out for controllers to legitimise a data processing, while such processing would not pass the legitimate interest test.

In summary, contrary to what is sometimes thought, our proposals do not necessarily mean that thus more data could be processed than is currently the case and that thus the existing level of protection would be undermined. It may well be the case that when the data minimization principle is applied in respect of the **interest** served with the processing rather than the **purpose** (think of the commercial health app in the example given) this would result in fewer data that may be collected and processed, or in certain cases even no data at all.

To avoid any misunderstandings, we here explicitly state that we are not in favour of a so-called *use-based* system. Under such a system, data collection is not subject to any restrictions, and only the use of data is regulated. Especially in the US, this system is often advocated as the most appropriate approach to regulation of data protection, now that in our data-driven society it would no longer be possible to regulate all forms of data processing. The idea is that the law-makers have no role in determining the conditions under which collecting and combining data may occur, but only in setting standards in cases where data are used in a manner that should be qualified as abuse (as an *unfair processing*). This approach is consistent with the regulation of advertising – advertising is in principle allowed, but misleading advertising is subject to sanctions. Although there is much to be said for such a use-based system, in our view it is necessary to continue to regulate also the collection of data. Without regulation of also data collection, we will quickly reach a situation in which governments and companies will collect data in an unwieldly manner– by e.g. placing *sniffers* in telecommunications networks, using the justification that the data so collected may possibly be of some use in the future. For this reason we consider that the collection of data should meet the legitimate interest test as proposed.

Our proposals are based on five pillars. These are ultimately all related to our observation that the current approach to the data protection undermines societal support for these legal rules. On the one hand, a large amount of data is processed in violation of the applicable laws, which are not enforced, even though citizens in fact object to these forms of data processing. On the other hand, the current legal framework prohibits the use of personal data for certain (especially big data analytics) purposes, even though some of these uses have clear societal value and the associated risks thereof are so limited that such uses ought to be permissible. In other words, the current legal framework does not reflect the reality of everyday life sufficiently in order to be effective and therewith be accepted as legitimate.

The **first pillar** is the observation that in the past, personal data were invariably a by-product of the purpose for which these data were collected. As a result the purpose limitation test served as an objective restrictive test in respect of the types of data that may be collected. Due to technological developments this is by no means always the case today. An example where data are collected as a by-product: when we book an aeroplane ticket at a travel agency, we are asked to provide our name, address, date of birth and bank details. The travel agency then uses this information to book the flight. These personal data are primarily a by-product of the purpose for which they have been collected: the service of booking the flight. In this situation, the purpose limitation requirement limits the types of data which may be collected for the relevant service. Asking customers for their religion, for example, is not necessary in order to book a flight and would therefore not be permissible.

The concept of purpose limitation relies on the premise that it is possible to decide on the purpose of a certain data processing beforehand. This while the added value of big data and the Internet of Things resides in the potential to uncover new correlations for potential new uses once the data have been collected. These new uses may therefore not have anything to do with the original purposes for which the data were collected. There may even not have been an original purpose; the data are often first collected in order to subsequently being able to decide on potential new services on the basis of an analysis of those data. Here the primary purposes are data collection and analysis, as a result of which the purpose limitation test no longer provides for an objective restrictive test for what types of data may be collected in the first place. Again an example to illustrate. Insurance companies collect data to analyse these as part of their search for new products and services. In this case, the primary purpose of data collection is simply to acquire data, and the data are by no means a by-product of providing another service (such as in the example of booking a flight). If data collection and analysis are themselves the purpose, purpose limitation is no longer meaningful (will no longer limit the types of data that can be collected). This is particularly true now that the data controller can itself determine the purpose and will invariably have a commercial interest in that purpose. In our view, the test should be whether there is a ‘legitimate interest’ in collecting and processing the data. Not only would all data controllers then have to state their **interest** in collecting the data, but they would also have to demonstrate that – given the relevant context – that interest is a **legitimate**. This will require a balancing of the various interests at stake, which should not only include the commercial interests of the data controller collecting and analysing the data, but also the interests of the individuals involved **as well as those of wider society**. Recent ground-breaking decisions by the ECJ, in particular the case of *Google Spain*, show that companies are now being instructed to indeed make such a broad assessment balancing all interests involved.

The **second pillar** is the belief that we must abandon the notion that data controllers are acting lawfully simply by virtue of the fact that they notify individuals and ask them to click ‘OK’, when at the same time they have no legitimate interest to process these data. Privacy legislation needs to regain its role of demarking what is and is not permissible. It is currently characterized by what we coin *mechanical proceduralism*, whereby data controllers notify individuals and ask for their consent in a mechanical manner, without offering effective data protection in practice. This observation is not new. We note that many authors and also EU legislators have concluded that citizens do not understand the information provided and blindly give their consent. What is surprising is that they then do not draw the obvious conclusion that the legal basis of consent should therefore be abolished, but instead start strengthening the information and consent requirements. We beg to differ here. A comparison with regulation of advertising and corporate marketing practices is pertinent here. Anyone is free to advertise their products and services, but misleading advertising and unfair commercial practices are prohibited. When applied to data processing, this approach would result in a regulatory framework within which data collection and processing is permissible if there is a legitimate interest, i.e. data processing which is deemed to be ‘unfair’ or ‘not legitimate’ will be unlawful. In the long term, such an approach could well prove itself better able to provide protection for individuals than the current system, which in effect tolerates a situation whereby consent can be asked for a processing for which there is no legitimate interest. To compare: nobody would dispute that it is not possible to request consent from consumers to receive misleading advertising or be subject to unfair trade practices. Such consent would not be valid.

The **third pillar** is the observation that individuals become more and more transparent, except for themselves. The reality of today's data-driven society is that individuals often do not know which data are being processed about them, how they are being assessed and categorized by the data controllers, and what the consequences of this might be for them. This is occurring despite the legal requirement of the controller to inform the individuals concerned, and the rights of individuals to access and correct their data. Under the existing regime, the information requirements are considered to be a cornerstone of privacy legislation, which is based on the assumption that individuals can only exercise their rights if they are aware that information about them is processed. The GDPR, which will become effective per 25 May 2018, is based on the same starting point: ‘Natural persons should have control of their own personal data’, and to this end imposes stronger requirements in relation to notification and consent. Our observation is that the current information and consent requirements are not effective. Although the new GDPR brings many improvements, the strengthening of the information and consent requirements will not improve the position of individuals, let alone give them a sense of greater control over the processing of their data. The underlying logic of data processing operations and the purposes for which these are used have now become so complex that they can only be described by means of intricate *privacy policies* that are simply not comprehensible for the average citizen, because of both their content and their excessive length. The result is that hardly anybody reads these privacy policies. This complexity renders individuals powerless and fosters indifference, with the result that many people simply click ‘OK’ when using online services. We will all recognize this phenomenon. Strengthening the information and consent requirements will therefore not help. On the contrary, this will result in even more impenetrable information, to be read by even fewer people.



It is an illusion to suppose that by informing individuals better about which data are processed and for which purposes, we enable them to make more rational choices and to better exercise their rights. We therefore need to depart from the existing system, which is based primarily on the notion that individuals themselves have to enforce compliance (on the basis that they are informed and have rights). Of course, individuals should have the possibility to defend their own privacy interests and the principle of transparency should facilitate them in this. However, allocating responsibility for enforcement primarily with individuals – as is the case under the current system – is not a desirable situation. A suggestion here is that legislators should extend *privacy-by-design* (including *security-by-design*) requirements also to suppliers of software and technical infrastructure, where they now apply only to data controllers (who have a commercial interest in the collection and processing of data). The effectiveness of e.g. the cookie-rules would be enhanced if users could choose their cookies settings via their web browser (of which there are currently five). The suppliers of web browsers would have no commercial interest in which cookies setting their users choose, and it would be easier to regulate these five providers than to monitor the countless parties that own websites and may decide to interpret the rules ‘creatively’.

The **fourth pillar** is the observation that the regime for special categories of personal data (health data, criminal data, religion, race and ethnic background, etc.), is no longer meaningful. Increasingly, it is upfront unclear whether data are sensitive. Rather, the focus should be on whether the use of such data is sensitive. Companies and the government use potentially ‘innocent’ data (some of which are freely available in the public domain) to make distinctions between individuals (discrimination) which may be very sensitive. One famous example is the Target-case, whereby the US retailer Target used big data analysis to send advertising for baby products to women who had suddenly switched to buying unscented cosmetics. This was because their data analysis had revealed a clear link between pregnancy and the purchase of these particular products. The data collected where in fact fairly innocent data (switching to unscented cosmetics), but the data were used to draw conclusions about an individual’s state of health - in this case pregnancy. That this use can be considered privacy invasive is shown by the fact that a complaint was lodged against Target by the father of a teenage daughter. Later it turned out that the girl was indeed pregnant, but that the girl had not yet told her father. There are further many types of data that do not fall within the ‘special categories’, but are undeniably sensitive because of the impact on individuals if they are lost or stolen. This includes passwords for access to IT systems and websites, credit card details, social security numbers, passport numbers, and so on. Furthermore, the sensitivity of data will often depend on the combination thereof, because they can be used for convincing *phishing* e-mails. For instance, an e-mail address is not in itself sensitive data, but in combination with a password it becomes highly sensitive – as many people use the same email/password combination to access different websites. The loss of this combination of data would pose a distinct risk to the individual concerned. Then there are situations in which non-sensitive data suddenly becomes sensitive when it is linked to data that may be indirectly sensitive, such as nationality, or postal code. Conversely, there are also plenty of examples where special categories of personal data are not sensitive in the context of the relevant processing purpose, as a result whereof there is no need for a stricter regime (such as higher security). For example, pension records include the name and gender of the partner of an employee, thereby revealing the sexual orientation of that individual. For the data controllers, the need for a special regime for just those data is not always self-evident.

Our observation is that it is the context in which data are used that is sensitive, more than the data themselves. As a consequence, the existing European data protection regime – which is based on the processing of special categories of data – does not achieve the intended effect. In some cases the regime is ineffective because the context in which sensitive data are used does not give rise to any particular implications for privacy. In other cases, the law does not provide the required additional protection because the regime for sensitive data does not apply, even though the context in which the data are used may justify more stringent requirements.

The central issue in all this is that the regime for the use of special categories of data does not include a check on whether there is a legitimate interest for that use. Under the existing regime, the legitimate interest ground is not available as a legal ground for processing special categories of personal data. Without listing all the various legal grounds for the processing of these special categories data, these consist mainly of the performance of specific contracts (e.g. health data may be processed insofar as this is necessary for the performance of an insurance contract), processing for specific purposes (for example, data on a person's race may be processed insofar as necessary for identification purposes) and further when the individual has provided his or her consent. What is problematic is that these legal grounds do not require a balancing of interests test, which test would include an assessment of the mitigating measures taken by the data controller to mitigate any adverse effects on the privacy of the individuals concerned. This assessment is deemed to have already been made by EU legislators when determining the appropriate legal grounds. In this respect, the legitimate interest ground, contrary to what many people believe, can actually provide greater privacy protection for individuals. Indeed, this has been acknowledged by the WP29 (Opinion WP29 06/2014, p. 9-10).

As far as special categories of personal data are concerned, the WP29 has overcome this problem by indicating that the protection of such data under Article 8 of Privacy Directive (the regime for special categories of data) should not be lower than if the processing had been based on Article 7 of the Privacy Directive (providing the legal grounds for the processing of ‘regular’ personal data). According to the WP29, the grounds in Article 7 of the Privacy Directive apply *cumulatively* if the protection under Article 8 of the Privacy Directive is lower (Opinion WP29 06/2014, p. 15-16). The WP29 therefore does indeed apply the legitimate interest test for data processing in certain cases. The position of the WP29 is understandable from a data protection perspective, but equally it is clear that the manner in which this is achieved is not optimal (adds to the legal complexity).

Under the GDPR, the specific regime for special categories of data remains in place. The shortcomings that we have just described (the lack of a balancing of interests in relation to certain grounds and the lack of the requirement for implementing mitigating measures) are (partially) offset by new requirements. For example, data controllers are required to perform a Data Protection Impact Assessment (**DPIA**) where a type of processing is likely to result in a high risk to the rights and freedoms of individuals (note that this is broader than privacy alone), and this is an explicit requirement in the case of large-scale processing of special categories of data. Additionally, data controllers must consult the supervisory authority prior to starting the processing where the DPIA indicates that such processing would result in a high risk *in the absence* of mitigating measures taken by the controller. Note here that the mandatory DPIA requires a contextual assessment, including an assessment of the necessity and proportionality of the processing activities, an analysis of the risks to the rights and freedoms of individuals and the mitigating measures that the controller envisaged to limit these implications. This analysis must therefore also be carried out if the legal ground for the intended processing of special categories of data is based on consent or execution of contract. In effect, these additional requirements are being introduced through the back door by means of the DPIA. Although this is quite understandable from the perspective of data protection, what concerns us here is that the manner in which the GDPR seeks to achieve this goal does not accord with the principles of good regulation (just adds to the complexity).

If our proposed legitimate interest test were to be applied, a special regime for special categories of personal data (health data, religious belief, ethnic background, etc.) would no longer be needed. The nature of the data and its potential use would be among the factors considered when applying the legitimate interest test.

The **fifth pillar** of our proposal is the observation that the current system for assessing a data processing is too complex for the data controllers to apply. Under the existing system a controller must demonstrate that **a.** there is an explicitly defined and legitimate purpose for its data collection and processing activities; **b.** that there is a legal ground for processing these data; **c.** that there is also a specific ground for processing special categories of personal data (and, if this test is less stringent than the test for regular data under b., then the processing must also meet the requirement under b.) and **d.** that any further processing of personal data is ‘not incompatible’ with the original purpose for which the data were collected. Our experience is that most controllers are not aware of the fine distinction between these different tests (and the different grounds). The system is simply too complex, and as a result the rules are often ridiculed instead that a serious attempt to comply with them is made. Since the system introduced in the GDPR remains unchanged in this respect, this criticism remains as valid as ever. We need to move towards **a single test** for all the various phases of the life cycle of personal data: collection, processing, further processing and destruction. This would represent a considerable simplification of the legal framework with a higher chance that the rules are actually adhered to.

In addition to the five pillars, our proposals are also based on a number of legal theories. The first of these is our view of the concepts of privacy and personal data protection. In situations where data controllers use our data, we often speak of an ‘intrusion of our privacy’. However, the legislature makes a distinction between respect for private life (privacy) on the one hand and protection of personal data on the other. The main reason for this distinction has been the difference in the function of the classic right to privacy on the one hand (a subjective right to keep certain private affairs outside the reach of third parties) and data protection law on the other hand (the various principles that dictate how data should be processed, in order to ensure the appropriate degree of care being taken into account given the interests of all the parties involved). Our observation is, however, that the innovative forms of data usage entail that the dividing line between these two concepts is becoming less clear-cut.

As humans, we need this degree of separation in order to form and develop our own personality and identity.

 “A life spent entirely in public, in the presence of others, becomes […] shallow. [I]t loses the quality of rising into sight from some darker ground which must remain hidden if it not to lose its depth in a very real, non-subjective sense”. Hanna Arendt, Quoted from: Solove, 2008, p. 164.

Both technological and social developments (combatting of fraud, counter-terrorism, the need for increased efficiency, service innovation, convenience, etc.) entail that the scope that we have to live our lives unobserved is diminishing. Simultaneously, the flood of new forms of intrusion into our privacy neutralizes the ‘taboos’ once associated with breaches of the legal framework. Previous indifference of ‘I have nothing to hide’ now seems to have given way to resignation: ‘I have to enter my personal *details, if I want to...’. Increasingly, it is seen as normal or inevitable that we become more transparent -* both in quantitative and qualitative terms - not only to the government and the private sector, but also when it comes to our friends and fellow citizens. Although privacy is enshrined as a fundamental right, and is formulated as the right to the protection of our personal sphere – which implies by its very nature the setting of boundaries – it seems that we are becoming ever more visible as individuals. This is beyond ‘just’ the monitoring of people. It is about the fact that governments and companies are increasingly able to steer social and economic processes using data. Our conclusion is that the distinction between privacy and data protection does not take account that also in respect of the right to data protection ultimately a clear and definite line must be drawn about what is or is not a justifiable intrusion. The system of data processing principles should not only serve to regulate the relevant bilateral relationship, but that law-makers will also need to define limits where data processing is not legitimate at all in the light of the collective interests that are increasingly at stake. Only then can justice be done to the constitutional anchoring of the protection of personal data at the EU level (Article 8 of the EU Charter).

Our proposals are also inspired by Fuller and Selznick, who developed the ideal that ‘legislators must adopt the perspective of those who have to work and live with the rules that they make’ (responsive regulation). We also call on the concepts that Witteveen once referred to as the ‘sense of realism’ and ‘sense of capability’ of legislation.We combine the ideal of responsive regulation with the belief that a society will have to ensure that privacy and data protection actually mean something to its citizens. And if it appears that governments need to play a much more active role than in the past, then the case must be made for doing so. We base this belief in part on the *capability approach* of Nobel Prize winner Amartya Sen. On the basis of Sen’s ideas, we arrive at the conclusion that data protection should be closely linked to the **capabilities** that people have in practice to realize a certain degree of private space for themselves. When applied to the areas of privacy and data protection, this means that the current procedural approach to data protection fails to provide sufficient guarantees. In concrete terms, this means that the existing legal framework whereby a data processing is assessed chiefly in terms of various principles that dictate how data should be processed (*fair processing principles*) to be applied in the relevant bilateral relationship between the controller and the individual involved – is no longer adequate. Our analysis shows that, in practice, this results in ‘moving the goal posts' rather than in 'setting limits'. In order to allow individuals to have a real opportunity to exercise their right to become a unique human being and to allow them sufficient scope to do this (in a physical and an informational sense), they must in fact also be empowered to do so. In any legal framework for data protection, the issue of **the permissibility of certain types of data use** must also be addressed. This must involve a consideration of not only individual interests but also of the collective interests that are at stake. Under our approach, the consent of individuals and the existence of a contractual relationship would no longer constitute independent grounds for legitimizing a data processing. In concrete terms, this may mean that some forms of data processing will no longer be permitted, even though they are currently in accordance with the law.

*Does the GDPR render our proposals obsolete?*

We are aware that the GDPR has now been agreed and published and that our proposals can no longer influence the GDPR. Moreover, our proposal to abandon the purpose limitation principle is not consistent with the Charter of Fundamental Rights of the European Union (**EU Charter**), which explicitly contains this criterion, and abolishing this criterion would therefore require a treaty amendment. Nevertheless, we believe that our thoughts and the concrete proposals that we present remain relevant. Firstly, we expect that the normative framework will ultimately develop along the lines that we describe. But in the shorter term too, the test that we have developed will be relevant. We will see that the compatible use test for the **further** processing of data (in essence, the **re-use** of data that is so vital for big data and the Internet of Things) will play an increasingly prominent role. The GDPR sets out the criteria that are to be used for this test. We note that these are almost the same criteria that had already been formulated by WP29. And these criteria, in turn, nearly fully overlap with the criteria that WP29 specified in relation to the assessment of the legitimate interest test. All tests involve an assessment of the data processing activities in the relevant context (in the light of the interests that are at stake), the proportionality of the processing and the measures taken to mitigate the privacy implications for those involved. It is expected therefore (as is also now the case) that the two tests will often produce the same result. Given the additional requirements that WP29 now places on the other legal grounds for processing – such as the processing of sensitive data– the conclusion is that for data controllers the most legally prudent method of operation is to use a uniform protocol (known in practice as a *Privacy Impact Assessment*) to carry out a contextual assessment of the implications of the use and re-use of data. This assessment ensures that their data processing activities are assessed according to the criteria of the legitimate interest test (and the compatibility test) and that the results of the assessment, as well as the basis for the decisions made, are documented. This method of working allows data processing to be assessed for legality using one single substantive test (rather than using a range of different legal criteria), while still complying with the new requirements under the upcoming GDPR.

The move to an assessment based primarily on legitimate interest would, in our view, be the first step in a transition towards a new approach to data protection. The regulation of data processing on the basis of the legitimate interest test will, in time, also prove insufficiently flexible. Instead of trying to set rules on data processing in advance, over time a system under which abuses are punished retroactively should be the next step. A comparison with the regulation of advertising and corporate marketing practices is pertinent here. Anyone is free to advertise their products and services, but misleading advertising and unfair commercial practices will be finished. Indeed, it is not feasible to incorporate all conceivable forms of advertising and trading practices into regulation on advertising, because these are constantly changing. The question of when exactly advertising is deemed to be misleading or commercial practices are deemed to be unfair, has become clear over time through case law and self-regulation. When applied to data processing, this approach would result in a regulatory framework within which data collection and processing is permissible, unless it is deemed to be ‘unfair’ or ‘not legitimate’ and therefore unlawful. This approach, too, would require controllers to carry out a contextual assessment and a balancing of interests in relation to their own processing activities, which would include an assessment of the possibility of unfair or unjust practices. And again, relevant for this assessment would be the extent to which controllers have taken mitigating measures to minimize any privacy and societal implications. If a judge were to find that a particular data-processing practice was unfair or not legitimate, then consumers would be entitled to compensation (strict liability). In the long term, such an approach could well prove itself better able to provide protection for individuals than the current system, which in effect tolerates a situation whereby personal data can be used for a 'fee' (i.e. in return for the online service that is provided), but this fee does not go any way to compensating the ultimate harmful effect of the use of those data. To compare: individuals would be able to consent to receiving misleading advertising or be subject to unfair trade practices.

In one of his columns, the Dutch writer Arnon Grunberg argued for the introduction of the ‘right to ignorance’ as a human right. Of course, democracy can only function if citizens are able to make informed and reasoned choices, says the writer. But equally, true knowledge requires specialization and not many citizens can spare the time that is needed to achieve this. ‘A decent society allows its citizens to be ignorant, if they wish, without that ignorance leading to allegations of immoral behaviour.’ We would like to extend his argument to an essential aspect of the developments described here. The idea that individuals have sufficient knowledge to take charge of the protection of their own personal data is naive. Knowledge is no longer an adequate tool when it comes to the ability to make deliberate, privacy-conscious choices. The ‘ignorance’ of citizens - for whom clicking ‘OK’ is, in practice, often the only option - should not imply, therefore, that their privacy may potentially be compromised. A decent society should allow its citizens the option of ignorance in this area, and equally it should allow them the option of making their own life choices and determining their own lifestyles. In other words, we must move towards a more modern system of privacy protection under which individuals - despite their inevitable ignorance - are assured certain legal rights when it comes to privacy, so that they continue to be free to grow, develop and make their own judgments.

At the same time, where individuals do wish to control their own data, the protection regime will still need to facilitate this. But more than that, law-makers must design a framework of norms that enables citizens to exercise their legitimate right to privacy in a meaningful way. To return to the example of the app that analyses health with which we started: for some of us, the right to privacy will come down to the fact that they want to know as much as possible about themselves. For others, by contrast, it means that they do not want to be told about their possible future state of health. The arguments presented show that in order to accommodate these varying interpretations of the right to privacy, the current – predominantly procedural – approach to data protection does not provide sufficient guarantees.