Prof.dr. Gerrit-Jan Zwenne

Diluted Privacy Law

Universiteit
Leiden
The Netherlands

Discover the world at Leiden University

Diluted Privacy Law

Paraphrased translation from Dutch of the
inaugural lecture by

Prof.dr. Gerrit-Jan Zwenne

on the acceptance of his position of professor of

Law and the Information Society

at the Universiteit Leiden

on Friday, April 12, 2013.

Universiteit
Leiden

Mr. Rector-Magnificus, my distinguished listeners!

Who cares about privacy?
"Who cares about privacy?" That's what Frank Kuitenbrouwer asked in an article in the NRC newspaper of 15 September 2007.[1] The main reason for considering this question was an article by two young researchers at this university, who had the temerity to say that privacy legislators were being too ambitious, that the scope of the privacy law was too broad, and that the rules of this law were sometimes too vague.[2]

"*It shows audacity to call the privacy laws too ambitious*," said Kuitenbrouwer. "*Will that ever apply to fundamental rights*?

Even now this question is still relevant. At this moment new privacy or data protection law[3] is in the making in Brussels. As a case in point, there is a proposal to widen the scope of this law. The current privacy law applies to data about persons whose identity is known or may be known. In the new proposal, this law should also apply to data that singles out, or differentiates, one person from another, without their identity being known.

This proposal is ambitious, and yes, perhaps even too ambitious. If the privacy law is to apply to all data which distinguishes one person from another, it will be hard to imagine situation in which the privacy law will not apply. The criteria for use of the law will be so ill-defined (that is to say, to ability to single out one individual from another) that its scope will almost be unlimited. One could call this the watering down or dilution of the privacy law.

Is this a bad thing? It is about fundamental rights, isn't it? It is a bad thing precisely because it is about fundamental rights. The consequence will be that we will somehow have to limit the scope of the law, and that will result in legal uncertainty. And this is what will make data protection and privacy law harder to apply than it already is.

This afternoon I will discuss the scope of data protection law, using IP addresses as an example. The question to be discussed is whether or not data protection law applies, or should apply, to IP addresses. This question, and the different answers that have been given in the recent past, provide insight into the lawmaker's aims and into the roles of privacy regulators. And this is what I would like to discuss with you today.

I will start with a short lecture on what personal data really are.

A short lecture on the concept of personal data
The privacy law applies to all personal data. Personal data are: "*any information relating to an identified or an identifiable natural person*". This is the definition given by the European Data Protection Directive 95/46/EC.[4]

The term 'identifiable', refers to "*[a] person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

From this it is difficult to assert exactly *what* the lawmaker means by the term 'identifiable'. It does say *how* to identify an individual: that can be done by the use of a number, or else through the recognition of certain features of someone's identity. The issue is if the person or organization that controls personal data (we call this person 'the controller'), or any other person using resources at his disposal, can within reason determine an individual's identity.

From Directive's recitals,[5] from parliamentary documents accompanying the Dutch Data Protection Act[6] and their associated literature,[7] I distil three important aspects.

Allow me to explain them:

1. Identity. The first aspect is the identity of the person associated with the personal data (we call this person 'the data subject'). The term 'personal data' applies when it is possible to use the data to ascertain the data subject's identity. Data are not personal data just because they say something about an individual, even uniquely so, rather because they refer to someone whose identity is known or can be known.

A telephone number, a number plate or a fingerprint are not in themselves personal data. But they may become so when combined with other data, such as with names and addresses from a telephone book, the names from the vehicle registry or a fingerprint database. This is because, with the exception of instances of spontaneous recognition, it is only through combining these different data that it possible to identify someone.[8]

I call this the 'aspect of identity'.

2. Reasonableness. Second is the aspect of reasonableness. There can only be personal data if-it doesn't cost a disproportionate amount of effort to ascertain the data subject's identity. If it *does* take a disproportionate amount of effort to ascertain the data subject's identity, while taking into account the means of identification that are at hand, there can be no identifiability. If this is the case, then the data are not personal data. The mere theoretical possibility of identifying someone is therefore insufficient to qualify data as personal data. It should not take an unreasonable amount of effort to do so.[9]

3. Relativity. The third aspect is one of relativity. In other words, some data may be deemed to be personal data to one person, whereas to another, the same data, at the same time, may not be deemed as such. The difference in aspect is determined by the possibilities that one person has, and another person not has, when trying to ascertain the data subject's identity.[10]

The aspect of relativity stands in relation to the aspect of reasonableness. A reasonable amount of effort for one does not have to be the same for another.

Perhaps an example can clarify this.

I have here a glass with a fingerprint on it. You can't see it, but I can. That fingerprint is not mine. I have not touched the glass because, as you can see, I'm holding it with a tissue. We don't know whose fingerprint it is. And that is why this fingerprint, even though it is certainly unique to a particular individual, is not personal data. This is what is meant by the identity aspect.

Perhaps someone can be identified using fingerprint, by a fingerprint database for example. But you or I cannot do this. We have no access to this database. Therefore, for us, it would demand an unreasonable amount of effort to determine the identity of the owner of the fingerprint. The aspect of reasonableness says that we do not have to treat this fingerprint, as personal data. And that is a good thing, as it would make doing the dishes unnecessarily complicated.

Obviously, this could be different for the National Forensics Institute in The Hague. I expect that the forensic specialists there have access to a fingerprint database. And without exercising an amount of unreasonable effort, these people can probably determine whose fingerprint it is. In that case, the fingerprint is personal data. But only for the institute, and not for us. That is what is meant by the aspect of relativity.

These three aspects make the definition of personal data dynamic and dependent on context. What may, at a given time, in a given situation, for a given individual be deemed to be personal data, may in another situation and for another person not be deemed as such. The three aspects determine when data

protection law applies, and in which situations. They make the law useful and give it meaning, and they contribute towards its effectiveness. In that sense these aspects are essential for the application of data protection or privacy law.

But at the same time it is these aspects that make the definition of personal data so complicated. In some cases it is hard to determine if personal data is involved. It always depends. And that is what always makes things difficult.

That ends my short lecture on the definition of personal data. I will now continue with the question of whether IP addresses should be considered personal data.

Are IP addresses personal data, or not?
IP addresses are the numbers assigned to Internet Service Providers (ISPs), which in turn assign them to their subscribers' computers, tablets and smartphones. IP addresses allow these devices to be found and recognized on the internet.[11]

So are IP addresses personal data or not? Often they are - but often they are not. It depends. Your IP address *is* personal data to your ISP. Why? Because your ISP can determine your identity without that much effort. Your ISP can do this because it has information about you, the subscriber, which corresponds to that particular IP address. So you can be identified by the ISP through your computer's IP address.

This may be different, however, if other people, such as your children, family members or roommates, use the same internet connection. It is unlikely that your ISP, or anyone else, will be able to determine the identity of these other users. And in that sense IP address is not personal data, not even for your ISP. Your ISP will not be able to identify the users with the help of its subscription data. The same thing happens when you make use of 'free internet' in the train or in the lounges at Schiphol Airport.

So, IP addresses are often personal data, but often they are not. It always depends.[12]

For a long time this take on IP addresses went undisputed, but this appears about to change. In particular, data protection authorities (DPAs) are playing a role that we without hesitation can call important. At first they agreed that IP addresses often qualified as personal data, and often as not. At this present moment they believe that IP addresses always and by definition must be qualified as personal data, and must at least be treated accordingly.

This is an important development. It is worth our while to consider why.

At the beginning of this century, the European consultative body of national data protection authorities, the so-called Article 29 Working Party, published a document on internet privacy. In this publication the Working Party determined that many IP addresses are only personal data for ISPs if the ISPs systematically record the dates, times and durations of use of the IP addresses. The idea was that, with this data, they could determine the internet users' identity without an unreasonable amount of effort.

The Working Party remarked that this would only apply to ISPs, and not to anyone else. There are occasions when it is possible to associate IP addresses with other data. However according to the Working Party that doesn't alter the identifiability of the internet user. It stated: "… *it might not be possible to identify a user in all cases and by all Internet actors from the data processed on the Internet*". In reference to the aspects of reasonability and relativity, the Working Party stated that IP addresses therefore often do not qualify as personal data.[13]

The Dutch DPA, the College Bescherming Persoonsgegevens, agreed with this point of view. At around the same time, the

authority released a press statement with the compelling title: "*An IP address is not always personal data*".[14]

In subsequent years, however, it has turned out that copyright holders in particular have been able to acquire subscriber information from ISPs through court applications. They were able to acquire information about subscribers corresponding to certain IP addresses where there was a suspicion that copyrighted material was being uploaded onto the internet. Consequently, these copyright holders could identify those subscribers. In such cases, according to an opinion of the Working Party published in 2007, these IP-addresses *are* personal data.[15]

Obviously, one could ask whether or not initiating such court procedures do not indeed qualify as a disproportionate amount of effort. Nonetheless, it is clear that the Working Party recognized that IP addresses are not always personal data as regards the aspect of reasonableness. The Working Party mentioned the internet café as an example: quite often in internet cafés it is not possible to ascertain the identity of the users.

So far nothing out of the ordinary. But then the Working Party came up with a different perspective, in - of all places - the very same advice. The Working Party determined that there is already identifiability when the use of the data "… *is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case*". And further, "*[i]t is sufficient if the individual may be treated differently from other persons as a result of the processing of such data*".[16]

All of a sudden, for the Working Party it was no longer a matter ascertaining the identity of the individual involved, but rather whether an individual can be categorized, and whether "[*i*]*t is possible to categorize this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him*".[17]

> It is most likely that the Working Party had in mind those internet users who cannot gain access to a particular website or service, because from their IP addresses it appears that they are from a certain country. You might be familiar with this if you have ever tried to watch a repeat of a television program on your computer in a foreign country. Quite often you can't access the program. This is because of your IP address: you are treated differently from other users, and that's without your identity even being known.[18]

In this interpretation of the concept of personal data, the Working Party ignores what I call the aspect of identity.[19] And, contrary to what has sometimes been suggested,[20] this means a radical new interpretation of the concept.

In the same advice the Working Party seems to limit the interpretation of the aspect of reasonableness. In the case of internet café users, the Working Party feels that IP addresses should be treated as personal data after all, even though internet users cannot be traced without an unreasonable amount of effort. However, because it is unclear which users can, and which users cannot be identified, the Working Party maintains that IP addresses should always be treated as if they were personal data anyway. It is no longer important to the Working Party that it may take an unreasonable amount of effort to identify the user. The Working Party stated that one can only conclude that certain data such as IP addresses are not personal data when the ISP is in a position to distinguish '*with absolute certainty*' that the data correspond to users that cannot be identified.

Here we see that the Working Party ignores the aspect of identity, and later the aspect of reasonableness. Six months on, the Working Party also neglects the third aspect, that of relativity, the one that determines if data can be deemed to be personal or not.

In an advice on internet search engines, the Working Party admitted that "*…[t]hough IP addresses in most cases are not directly identifiable by search engines,*" and that "*identification can be achieved by a third party …*" referring to 'law enforcement and national security authorities' and 'private parties in some Member States' (e.g. copyright holders). Because these third parties are considered to be able to ascertain the identities of users, the Working Party felt that search engines 'consider' IP addresses to be personal data, even if the search engines themselves do not have the means to identify data subjects. So the aspect of relativity no longer has any meaning to the Working Party either.[21]

These and other opinions[22] show that the Working Party now finds that IP addresses *always* qualify as personal data. And this is also the position that the Dutch DPA has taken. In a press release concerning the advice on search engines, the CBP stated quite clearly, that "*now, unambiguously, it has been established that IP addresses are personal data*".[23]

Much has changed in the attitudes of regulators concerning personal data and IP addresses. At first, their developing views didn't draw a lot of attention, perhaps because the Working Party's opinions are not everyone's bedtime reading. Nonetheless, from discussions about the new general regulation on data protection, we can see that regulators have started to expound their new dispositions with zest.

The proposal for a new regulation on data protection

The proposal for the new General DP Regulation is based on same definition of personal data as adhered to at present. In the proposal's definition the criterion is whether someone can be identified or not. And reasonably means to that end still need to be available. The proposal recognizes that IP addresses can be used to identify individuals, but does emphasize that IP addresses are *not* personal data in every situation.[24]

Amongst the reactions to the proposal, we can see that a digital rights group was the first to denounce this[25] with regulators and politicians following later on.[26] Their argument is that the regulation should apply when data is being processed from which individuals may be distinguished from others. For them it is no longer about identifying, but about individualizing, which is to say, 'singling out', or 'isolating' the individual.[27]

An interesting point in all this is that the Working Party maintains that identification automatically encompasses individualization, thereby suggesting that IP addresses were *always* to be qualified as personal data, a notion that cannot stand in light of its previous opinions. Others simply argue that the definition of personal data should be broadened, so as to recognize that identifying and individualizing are not the same thing.

Dilution of the privacy law

But what is one to think of that? What is one to think of broadening the definition of personal data? It might come as no surprise to you that I have some concerns in relation to this. I will now take you through five of these.

1. Limiting and defining. My first concern involves the three aspects I've just mentioned. In the Working Party's broader definition of personal data, the aspect of identity has been left out altogether. Little or no value is given to the aspects of reasonableness and relativity. As a result the definition of personal data becomes less dependent on context and also less dynamic. At first glance this would seem appealing, implying that the question of whether or not personal data are involved is an easy one to answer: the answer will almost always be that personal data *are* involved. Or at least, it will not be possible to exclude this premise. Unsatisfactory answers such as "it depends" and "often yes, but often no" will be confined to history.

In contrast, however, data protection law will apply in many situations where it is not needed. Exceptions will have to be made. Even the advocates of a broadened definition of personal data admit this. Because we are not at all certain that we can fit or work these exceptions into the law, more often than not we may expect reliance on what is called 'a reasonable application of the law' or else 'a sensible and flexible application' of it.[28]

This, in itself, is not new. Even the current data protection law sometimes goes far beyond its purpose. With the instrument of the 'reasonable rendering of the law', the Dutch DPA has made several attempts to bring the scope of the law back to what is still within reason. Up till now, these attempts in particular have introduced a lot of legal uncertainty, notwithstanding the captivating discussions they have generated.

Example no. 1. In its internet guidelines of December 2007, the Dutch DPA found it within 'a reasonable application of the law' to consider recognizable photos and video images only as racial data (as specified in article 16 of the Dutch Data Protection Act) if they are published with the explicit intent to make a racial distinction. However, in its decision of 23 March 2010 (LJN BK6331), the Dutch Supreme Court dismissed this interpretation.[29]

Example no. 2. The same internet guidelines mentioned several criteria to be used to determine if personal data are processed for journalistic purposes. A year after these guidelines were published, the criteria proved to be outdated after the decision by the Court of Justice of 16 December 2008, in the Markkinapörssi case.[30]

Example no. 3. In the spring of 2009 the Dutch DPA came up with a limited interpretation of article 4(1) of the Dutch Data Protection Act that deals with the territorial scope of the law. A mere two years later, the Article 29 Working Party came up with an opinion on the matter, which was, not surprisingly, a contrary view.[31]

It is important to know that data protection law already has many open concepts. It couldn't be any other way because the law has to be applicable in many different situations. The privacy legislator presumed that these open concepts would be filled in by sectorial legislation, court decisions or self-regulation.[32] The official evaluations of data protection law, however, have shown that this has not happened.[33] If only for this fact alone, I find it unwise to propose that in the next generation of data protection law definitions will be used that are even less distinct.

This is my first concern with regard to the broadening of the definition of personal data.

2. Foreseeability. A second concern deals with the foreseeability of the data protection law's rules, which is to say foreseeability as the term has developed through case law of the European Court of Human Rights. A broadened or stretched-out definition of personal data means that in many situations it will not be so straightforward as to whether or not the law is to be applied, and what that will mean for the controllers and data subjects. The scope of the law will be indefinite, or at the least it will not be possible to define its scope with certainty.

This makes adhering to the law, and also enforcing it, highly perilous indeed. To enforce a rule, and to be able to impose a sanction on a violation of that rule, it must have been made clear to the violator beforehand what was expected of him and which rules were to apply. Broadening the definition of personal data will make this very difficult in many situations, if not impossible.[34]

3. What are the considerations? A third concern deals with the substantiation of the need to broaden the definition of personal data, or rather, with the lack of such substantiation.

At present there are rules concerning IP addresses.[35] And indeed perhaps there are reasons to create more rules. And

perhaps there are reasons why the scope of the definition of personal data should be broadened even further. However, it is disturbing to think that the reasons for such broadening have either not been expressed at all or only cursorily.[36]

> The considerations as to why the definition of personal data should be broadened, are tenuous at best. LIBE-rapporteur Albrecht is content with the mere justification that "*[t]he concept of personal data is further clarified with objective criteria. Identifiers that have a close relation to a natural person must be regarded as personal data*".[37]
>
> The so-called Elissen Resolution, as adopted by the Dutch parliament, requests that the government broaden the definition of personal data, because "*the definition of personal data forms the nucleus of the new regulation […] and that this should be attained with utmost care*".[38]

The Working Party is limiting itself by referring to a *selection* of its own opinions and expressing its wish that DPAs should have a say in the use of IP addresses. These are teleological and authority arguments - in themselves not very convincing at all. "*The reason is*," to paraphrase the Working Party and DPAs, "*because we said so*", end of story.[39]

It is also not very convincing that the reasons presented by the Working Party are largely based on assumptions. One is that data protection law will offer more security and safeguards, simply by enlarging the scope. Is this actually the case? Would it really be that simple? I wonder. I think more is needed. Before we move on to expanding the scope of the law this should first be clarified.

4. The system or principles of the law. My fourth concern is about the principles of the law itself.

Data protection law is itself based on the idea of identified individuals. If, for example, someone wants to make use of his or her subject access rights, the controller has to establish the identity of the one requesting access.[40] This will be difficult - if not downright impossible - when it concerns access to data about individuals whose identity is unknown. What is the value of access rights in such a situation?

And what about informing the data subjects, one of the core obligations under the law? How can that be done when the data subjects are not known?

5. Evaluations. A fifth, and for the moment at least, final concern, is about the evaluations of the law that I have already mentioned.

These show that the unclear definitions of legal terms are a major problem, potentially the greatest problem of the law. It is annoying, if not disturbing, to see that no attention is paid to these evaluations in the discussions on the definition of personal data.

But perhaps I'm taking all of this just a little too personally. You shouldn't think that I've mentioned these evaluations because at the time I, along with my eLaw colleagues, contributed to them.[42]

I have highlighted but a handful of concerns. There are more. I could mention, for example, the subsidiarity principle,[43] or else the legitimacy of the DPA's decision-making. But I think you get the picture. It is not a good idea to simply broaden the scope of data protection law. There is a serious risk that this will lead to a dilution of data protection or privacy law, in the sense that the law will apply to everything and nothing, making it a law without meaning. We should not want that and neither should the legislator.

And with that I have come to the legislator's aims.

The privacy legislator's aim

When it comes to privacy, the privacy legislator has always been ambitious. The privacy legislator lays down rules for all sorts of activities: the very mundane as well as the common; for the important and the unimportant; for all kinds of social, cultural and economic activities. In the information society everyone, bar none, has to deal with privacy and data protection law. If not as a data subject whose data is being processed, then as the controller who determines how that is to be done.

Privacy and data protection law is about fundamental rights. And this is the reason why a lot of attention should be paid towards the quality of its rules. My point is that one should expect data protection law to be comprehensible, much more so than what we might find acceptable with other laws. At any rate, considerable attention should be given to the means by which its as yet undefined concepts are defined and clarified.

If this were a law that was relevant only to a handful of people, the legislator could perhaps allow itself to think up rules that are less easy to comprehend. For those parties involved - including regulatory authorities, courts and judges - it is to be expected that they take the trouble to understand them. For instance, we may expect telecom providers to delve into the incomprehensibilities of telecoms-law-related cost-orientation requirements.[44] And if that takes any effort, it will not be insurmountable, given the limited number of telecoms providers there are and the available resources at their disposal.[45]

As for privacy and data protection, this is different. Data protection law concerns us all, which is why this law should be understandable to us all. The definitions used should be evident without needing an unreasonable amount of effort to try to understand them. If there were such a thing as law not meant for 'specialists' or 'super specialists', then it should be data protection law.[46]

The desire to broaden the definition of personal data is at odds with this. The aims of the legislator should not be to widen the scope of the law to infinity and beyond, but rather to make it more comprehensible, useable and workable; to make it easier to regulate and enforce. Only then can it do what it is meant to do, namely to protect our privacy.

And the role of the data protection authorities

I've already said a lot already on data protection authorities. You may have got the impression that I do not appreciate what they are doing.

That is not the case.

The Dutch DPA, perhaps one of the best data protection authorities in the Netherlands, has assumed the role of explaining data protection law. As a case in point, the DPA has contributed significantly to clarifying the law. And that, of course, demands our respect.

But clarifying and explaining data protection law is not an easy task. A DPA that wishes to be credible should do its utmost to explain its reasoning, or at least it shouldn't mind doing so. And that is exactly what is missing in the discussion on personal data and IP addresses. The Dutch DPA is hesitant to admit that its position is subject to an ongoing process, and it is reluctant to explain why its views have changed.

This is very unfortunate indeed, as it makes a worthwhile discussion unnecessarily complicated and a serious debate impossible. To allow for a convincing contribution to explanation and clarification of data protection law, the DPA must allow for a meaningful discussion of its standpoints and their evolution in a wider arena, so not only with other DPAs and others who are like-minded.

Privacy is ours. The discussion about privacy concerns all of us. For those who care about privacy, this is self-explanatory. Or at least it should be.

Closing words

And so I come to the end of this lecture. According to the instructions I have received, it is customary - but not required - that at the end of his inaugural lecture, the professor express his gratitude, which I shall gladly do.[1]

I would like to thank the Executive Board of the University and the Board of the Faculty, the Rector Carel Stoker, in particular, and the Dean Rick Lawson, for the trust they have placed in me. I would also like to thank everyone else who has contributed to my appointment.

I will follow in the footsteps of Hans Franken and Aernout Schmidt. From my first tentative steps into the world of academia they have been - and indeed still are - my great, and often inimitable, examples. Hans, Aernout, many thanks!

I also owe my thanks to my other eLaw colleagues. I shall no doubt be leaving out a lot of people, but I hope that by naming a few I will make good on this shortcoming. In no particular order these are: Bart, Bibi, Franke, Jaap, Jan-Jaap, Martijn, Rob, Tess, Wouter, and of course Simone with whom I share the professorial chair.

It is not an easy thing to strike a balance between my work as a lawyer and my academic activities. I am grateful to my colleagues at Bird & Bird for having given me the opportunity to allow me to do both for more than twelve years already. I will doubtless be missing out on a lot of people once again, but I would like to name two in particular: Marjolein Geus and Ella Meijaard, who in their own ways have both been instrumental to my well-being at the office.

I am pleased to see in the audience several students who are following the courses in telecoms law and internet law. I look forward to exploring with you what can be done, what has to be done, and what should be done in the information society. You may not realize it, but there is a great demand for legal professionals with this specific branch of knowledge.

Last, but by no means least, my thanks also go, of course, to my family, especially those sitting here in the front row. For reasons involving protection of my and their privacy, I shall not go into details. At least not from this pulpit.

Querida Geidy, por razones de privacidad no puedo explicarlo ahora, pero sabes que estoy muy feliz de que estés aqui, porque eres la persona mas importante para mí.

I have spoken.

Notes

1 F. Kuitenbrouwer, 'Wie geeft er nog om privacy?', *NRC Handelsblad* 15 september 2007, opgenomen in: F. Kuitenbrouwer, *Recht en vrijheid*, Uitgeverij NRC-boeken 2010, p. 141-143 (in Dutch).

2 L. Mommers & G-J. Zwenne, 'Privacywetgeving is zelf het probleem', *Financieel dagblad*, 31 mei 2007.

3 In this lecture I will use the terms privacy and data protection law as synonyms. In my experience these terms are well understood and do not need further clarification.

4 Art. 2(a) of Directive 95/46/EC.

5 Recital 26 Directive 95/46/EC.

6 *Parliamentary documents II* 1997/98, 25 892, nr. 3, pp. 48-49, nr. 13, p. 2.

7 J. Holvast, *Persoonsgegevens of niet: dat is de vraag*, Samsom Bedrijfsinformatie bv, Alphen aan den Rijn/ Diegem 1996, pp. 3–103; G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer: Kluwer 1995, pp. 524-541; Van Esch, *Juridische aspecten van elektronische handel*, tweede Deventer 2007, pp. 75-76; K. Koelman & L. Bygrave, *Privacy, Data Protection and Copyright,* Amsterdam 1998; T. Oudejans, 'Internet on line. Privacy off-site', *Privacy & Informatie* 1998/4, pp. 153-160; R. van Esch & P. Blok, 'Privacy en elektronische handel via internet' in J. M. A. Berkvens & J. E. J. Prins, *Privacyregulering in theorie en praktijk*, Deventer 2007, pp. 205-206; T. Wisman en M. van der Linden-Smith, 'My secret life as an average person', *Tijdschrift voor Internetrecht* 2008, nr. 4, p. 88. Another viewpoint is defended by H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer 2011, pp. 64-65 (all in Dutch).

8 There is a lot of case law confirming that a number or a code, and sometimes even a name,cannot alone, but in combination with other data, can be used to identify a data subject. Cf. ECoJ 6 November 2003, case C-101/2001 (Lindqvist), nr. 24: "*The term 'personal data' used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, 'any information relating to an identified or identifiable natural person'. The term undoubtedly covers the name of a person <u>in conjunction</u> with his telephone coordinates or information about his working conditions or hobbies.*" (emphasis added); ECoJ 24 November 2011, case C-70/10 (Scarlet/Sabam), nr. 51 "*those [IP] addresses are protected personal data because they allow those users to be precisely identified*"; see further Dutch Supreme Court, 4 September 2012, *LJN* BX4153 or *Parliamentary documents II* 1991/92, 22 694, nr. 3, p. 3.

9 *Parliamentary documents II* 1997/98, 25 892, nr. 3, p. 47.

10 G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer 1995, pp. 526-527, 534, and footnote 1836 (in Dutch).

11 RFP760 (January 1980) defines an IP address as "a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication".

12 In 2013 a study on the qualification of IP addresses in Member States' and EU courts was published. It presented an interesting but, at least for Dutch and EU courts, not very accurate overview of case law. See Time.lex, "Study of case law on the circumstances in which IP addresses are considered personal data", D3. Final report, 2 May 2011.

13 Working Party Art. 29, Privacy on the Internet - An Integrated EU Approach to On-line Data Protection, (WP37), 21 November 2000, p. 22.

14 CBP, 'Een IP adres is niet altijd een persoonsgegeven', 19 maart 2001, z2000-0340 (in Dutch).

15 Working Party Art. 29, Opinion 4/2007 on the concept of personal data, (WP136), 20 June 2007, p. 17.

16 Working Party Art. 29, Opinion 4/2007 on the concept of personal data, (WP136), 20 June 2007, p. 17.

17 Working Party Art. 29, Opinion 4/2007 on the concept of personal data, (WP136), 20 June 2007, p. 11.

18 CBP Richtsnoeren, 'Publicatie van persoonsgegevens op het internet', 11 December 2007, p. 9. Zie ook CBP Definitieve bevindingen onderzoek 'Geen Stijl IP-checker' op www.geencommentaar.nl, kenm. z2008-01174, 27 October 2008 (all in Dutch).

19 The Working Party seems to confuse 'the user' and 'the computer used', and 'identity' and 'personality'. In this context the Working Party distinguishes between 'identity in a narrow sense' and 'identity in a broad sense': "*… computerised files registering personal data usually assign a unique identifier to the persons registered,*

in order to avoid confusion between two persons in the file. Also on the Web, web-traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name." Working Party Art. 29, Opinion 4/2007 on the concept of personal data, (WP136), 20 June 2007, p. 14.

20 Cf. EC Press Release: EU Data Protection: European Parliament's legal affairs committee backs uniform data protection rules, MEMO/13/233 Brussels, 19 March 2013.

21 Working Party Art. 29, Opinion 1/2008 on data protection and search engines, (WP148), 4 April 2008, p. 8; Working Party Art. 29, Opinion 4/2007 on the concept of personal data, (WP136), 20 June 2007, p. 17.

22 Working Party Art. 29, Opinion 13/2011 on Geolocation services on smart mobile devices, (WP 185) 16 May 2011, p. 11: "*The fact that in some cases the owner of the device currently cannot be identified without unreasonable effort, does not stand in the way of the general conclusion that the combination of a MAC address and a WiFi access point with its calculated location, should be treated as personal data.*"

23 CBP, 'Internetzoekmachines moeten privacy respecteren', 7 April 2008 (in Dutch).

24 Recital No. 24 of the proposed regulation.

25 Bits of Freedom, Letter of 2 March 2012 to the members of parliamentary committee on Security and Justice regarding the proposal for a general regulation on data protection (in Dutch).

26 *Parliamentary documents II* 2012/13, 32 671, nr. 31, p. 2 en 15; *Parliamentary documents II* 2012/13, 32 671, nr. 37; *Parliamentary documents II* 2012/13, 32 671, nr. 42, p. 5; *Parliamentary documents I* 2011/12, 33 169, C, p. 21.

27 G-J. Zwenne, 'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren', *Tijdschrift voor Internetrecht* 2011/1, pp. 4-9; G-J. Zwenne, 'Regulering van IP-adressen (en andere mogelijke identifiers)', *Tijdschrift voor Internetrecht* 2011/2, pp. 40-43 (all in Dutch).

28 See the remarks of Hustinx in J. E. J. Prins, 'Acht gesprekken over privacy en aanpalende belangen', in H. Franken e.a., *Zeven essays over informatietechnologie en recht*, Den Haag 2003, p. 69-73 (in Dutch). It seems these remarks echoed four years later in the Working Party's opinion on the concept of personal data: "*It is a better option not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data.*" A more nuanced and more reasonable approach is presented by the UK Information Commissioner in its 'article-by-article analysis paper': "*There is clearly considerable debate about whether certain forms of information are personal data or not. This is particularly the case with individual-level but non-identifiable - or not obviously identifiable data - such as is found in a pseudonymised database. We prefer a wide definition of personal data, including pseudonymised data, provided the rules of data protection are applied realistically, for example security requirements but not subject access. If there is to be a narrower definition it is important that it does not exclude information from which an individual can be identified from its scope. However, it is important to be clear that a wide definition plus all the associated rules in full would not work in practice. This is a real issue in contexts as diverse as medical research and online content delivery.*" Information Commissioner, Proposed new EU General Data Protection Regulation: Article-by-article analysis paper, V1.0 12 February 2013, pp. 6-7. See also C. Cuipers & P. Marcelis, 'Oprekking van het concept persoonsgegevens: beperking van privacybescherming?' *Computerrecht* 2012/187 (in Dutch).

29 Cf. CBP Richtsnoeren publicatie persoonsgegevens op internet, 11 December 2007 vis-a-vis HR 23 maart 2010, *LJN* BK6331; G-J. Zwenne & L. Mommers, 'Zijn foto's en beeldopnamen 'rasgegevens' in de zin

van artikel 126nd Sv en artikel 18 Wbp?', *Privacy & Informatie* 2010/5, pp. 237-247; CBP Richtsnoeren Identificatie en verificatie van persoonsgegevens: gebruik van 'kopietje paspoort' in de private sector, July 2012, p. 13 (all in Dutch)

30 ECoJ 16 December 2008, Case C-73/07 ("Markkinapörssi"); De Vries in *Tijdschrift voor Internetrecht* 2009/1, pp. 48-50 (in Dutch).

31 E. M. L. Moerel, 'Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008/3, pp. 81-91, M. A. H. Fontein-Bijnsdorp, 'Art. 4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/6, pp. 285-289, E. M. L. Moerel, 'Art. 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008-6, pp. 290-298; G-J. Zwenne & C. Erents, 'Reikwijdte Wbp: enige opmerkingen over de uitleg van artikel 4, eerste lid, Wbp', *Privacy & Informatie* 2009/2, pp. 60-67; C. M. K. C. Cuijpers, 'Toepasselijk privacyrecht in de wolk', *Computerrecht* 2011/65 (all in Dutch); Working Party Art. 29, Opinion 8/2010 on applicable law, (WP 179), 16 December 2010.

32 *Parliamentary documents II* 1997/98, 25 892, nr. 3, p. 6; *Handelingen I* 1999/2000, 34, p. 1605.

33 G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer 1995; G-J. Zwenne e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens, WODC 2007; H.B. Winter et al, *Wat niet weet, wat niet deert*, WODC 2008 (all in Dutch).

34 The Court ruled "*a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable citizens to regulate his conduct: he must be able- if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entaila*", ECHR 26 April 1979, 6538/74.

35 For example, in the Dutch Telcommunications Act, art. 11.2a, 11.5 and 13.2a Tw.

36 A text endorsed by '62 leading senior academics' gives some substantiation. This text does not however argue that the concept of personal data should be broadened, but that the regulation should also apply to data other than personal data. S. Spiekermann et al, 'Data Protection in Europe: More than 60 Leading European Academics are taking a position', 7 March 2013.

37 Jan Philipp Albrecht, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Committee on Civil Liberties, Justice and Home Affairs (COM(2012)0011), Amend. 15, 28 en 84.

38 *Parliamentary documents II* 2011/12, 32 761, nr. 37.

39 Working Party Art. 29, Opinion 01/2012 on the data protection reform proposals, (WP191), 23 March 2012, pp. 9–10.

40 Art. 37(2) Dutch Data Protection Act; art. 15(4) of the proposed regulation.

41 G-J. Zwenne e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens, WODC 2007 (in Dutch).

42 In par. 3.2 of the explanatory memorandum of the proposal aims to justify why a regulation is needed. A question to be answered is if, in view of the proposed broadening of the scope of the regulation, this still suffices. See also *Parliamentary documents II* 2011/12, 33 169, C, pp. 18-19 (in Dutch).

43 Cf. CBb 26 September 2012, *AB* 2013/22 (in Dutch).

44 Cf. C. J. M. Schuyt, *Op zoek naar het hart van de verzorgingsstaat*, Leiden/Antwerpen 1991, p. 215 (in Dutch).

45 Cf. Parliamentary documents II 1991/92, 22 694, nr. 3, p. 3; Parliamentary documents II 1997/98, 25 892, nr. 5, p. 6; E. Schreuders & H. Gardeniers, 'Materiële normen: de kloof tussen de juridische normen en de praktijk', *Privacy & Informatie* 2005/6, pp. 260-262; G. Overkleeft-Verburg, *De Wet persoonsregistraties* (diss. Tilburg), Deventer 1995, p. 527; G-J. Zwenne e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens, WODC 2007, pp. 72-73, 116, 126 (all in Dutch).

46 For their useful and valuable comments on draft versions of this lecture I owe gratitude to: Bart van der Velden, Bibi van den Berg, Laurens Mommers, Aernout Schmidt and Jos Webbink. Chris Weterings translated the text into English.

Prof dr. Gerrit-Jan Zwenne (Velsen, 1966)

2011	full professor law and the information society Leiden University
2006	partner Bird&Bird LLP
2004	associate professor Leiden University
1992-1998	assistant professor and PhD-researcher at Leiden University
1986-1992	Leiden Law School

On 1 October 2011, Gerrit-Jan Zwenne was appointed as full professor law and the information society at eLaw@Leiden, centre for law in the information society of the Leiden Law School. He specialises in internet, telecoms and privacy law.

Before, Gerrit-Jan Zwenne already held a position as assistant professor and associate professor at eLaw@Leiden. He read law in Leiden en was awarded his doctorate in 1998 at the same university for his thesis on taxation and information obligations. He gives lectures and courses in his areas of expertise and regularly publishes about these topics. In addition to his appointment at eLaw@Leiden he is partner at the international law firm Bird & Bird LLP in The Hague.

In his inaugural lecture Zwenne discusses privacy and data protection law on internet, particularly if and to what extent that law applies, or should apply, to IP addresses and other online identifiers. In this context he discusses the ambitions of privacy legislators and the role of data protection authorities in the information society. Ha argues that the legislator should not have the ambition to broaden the scope of the privacy and data protection law to infinity and beyond. The privacy and data protection law must be made comprehensible, workable and enforceable, and in with respect to this data protection authorities play an important role. This is why they should exert themselves to explain why they interpret the law the way they are interpreting it.

Universiteit
Leiden