INTERNATIONAL REVIEW OF LAW COMPUTERS
& TECHNOLOGY, VOLUME 11, NUMBER 2, PAGES 193–202, 1997

CARFAX

*Privacy as a Theoretical and Practical Concept**

PETER BLUME

The purpose of this article is to consider some general questions related to privacy and data protection. These legal concepts are viewed as aspects of justice which can be described as the primary goal of the legal system. Besides all the interesting and complex practical issues that are connected to data protection it is occasionally expedient to move up a level and take a look of the general nature of this part of the law. In Europe, where the main event currently is the implementation of EU directive 95/46, such a general approach can be helpful for an understanding of the problems facing legislatures. Also for the global development of data protection such a perspective is fortunate. As indicated below such theoretical considerations should be enhanced in the future.

First and foremost this article is concerned with privacy, a well-known legal concept and a right that is included in the traditional human rights catalogue. Privacy can also be seen as one of the values that constitutes justice. There are numerous theories of justice. In some, privacy plays a role and in others this is not the case. It is not the aim to analyse these theories, but just to demonstrate that in today's society some form of privacy must be a part of justice. A society in which people cannot in any way be themselves can from this point of view not be described as a just society. Although this article covers a broad scope of issues, including some of a primarily practical nature, it is also meant as a modest contribution to the general discussion of justice. In some sense this is not odd, as many theories of justice also cover a wide range of topics. As justice to a large degree is concerned with living conditions in a broad sense, it is fairly clear that justice cannot exclusively be a theoretically construed concept, but must be founded on observations of human behaviour. This again means that caution should be taken with respect to very abstract formulations of justice. They can be so imprecise that they lose their sense of meaning.

This article is accordingly based on the assumption that no single concept can describe or denote justice but that it is comprised of a series of concepts or ideas that together can demonstrate whether a certain society is just or not. The sum of human rights is important, but it is not certain that these are sufficient to constitute justice. This implies that justice is not an unambiguous concept—there is no correct nor true definition of justice. It depends on the historical period and the societal conditions, the values of which constitute justice. As well be demonstrated, privacy is a value that for most of human history has had minor importance, while it today is a basic part of the values that sustain justice.

*The article is a revised and amended version of a paper to be presented at the world congress of legal and social philosophy, Buenos Aires, August 1997.

Correspondence: Professor Peter Blume, University of Copenhagen, Faculty of Law, Studiestradede, Copenhagen, Denmark.

1360-0869/97/020193-10

In these opening remarks general questions will be in focus, while more specific remarks on privacy are reserved to later sections. Here is it interesting first to consider what a legal concept is. As a starting point it can be noted that concepts belong to theory and not to practice. Legal concepts can be useful in practice as they make it easier to identify and solve practical conflicts, but they are not phrased on or derived directly from practice. It must be added that this does not preclude that also practitioners can develop a legal concept. However, these are the result of theory they belong to the main core of theory. It is interesting to consider how a concept is born and how it is given influence. These questions seem to be fairly easy. A concept is developed by lawyers as a means either to describe a certain legal problem area or to enhance an idea that comes from the sphere of legal policy. Concepts can be powerful, as they provoke the human mind and underline aspirations and thoughts. One of the most powerful concepts is actually justice even though this as mentioned is not one single concept. No one will be happy to admit that he is unjust. On the general level, phrasing of concepts is probably the most important activity and can be viewed as the propaganda of theory. The purpose of an article such as this is accordingly to look behind the concept of privacy and to evaluate whether it can serve a beneficial function in society.

Another key element is legal culture. General concepts function within such a culture. Within legal circles it is fairly new to talk about culture as it traditionally has been concepts as law and legal system that have dominated the discourse. It should with this background be considered what a legal culture is. This is not easy as it is a broad and ever-changing concept.

A possible description could be that legal culture is the way in which people[1] think about law and legal issues. In a certain nation there will be characteristic ways to conceive law and they may differ from the beliefs in another state. The formal instruments and institutions might be the same, but the differences in the culture imply that the law works or functions in different ways. This again means that it is essential for the understanding of the law of state that the legal culture is understood. This is, of course, a major problem for comparative law that has to go behind the scenes. The notion of culture creates many problems also for legal theory which, however, should be welcome, because they can enable the theory to become more realistic and especially to understand that general concepts might not be universal but actually linked to specific legal cultures.

An additional complication is the fact that there may be several legal cultures within a state, the development of multi-cultural societies thereby becoming a complicating factor. This is the case in many EU member states. With respect to the implementation of the EU directive on data protection (see in Section 5) it is accordingly not sufficient just to transpose the directive into national law; it must also be diffused to the different cultures within the state. This problem area should be studied carefully in the future. However, for the sake of simplicity this article is based on a 'one state—one legal culture' approach.

Another way to explain legal culture is to describe it as an inside approach to law. Legal culture is not (directly) in the books of law and it cannot sufficiently be studied in those books. A legal culture has to be experienced, and this cannot take place outside the field of a specific legal culture. A basic scepticism towards international law in the sense of uniform law follows from these observations. Also the idea of comparative law seems to be doubtful. It is accordingly maintained that inclusion of legal culture as a basic ingredient for the understanding of law implies that there are no universal legal concepts today. Although it could be argued that this is an empirical question it is here seen mainly as a theoretical topic.[2]

The study of privacy must respect this observation and remember that both privacy and its modern variations function divergently in different legal cultures. For this reason the following pages should be read mainly as a Western approach, with the starting point in developments in Western Europe, although it should be added that also here there are major differences at the legal regulation level. As elaborated in Section 5, diverging legal cultures must be acknowledged as a problematic feature in connection with the EU data protection directive.

2. Privacy as a general value

The idea of privacy—that a sphere of a person's life is private—arises when technologies that can be used to infringe private life are developed. Before that time there does not seem to have been much concern about the borders surrounding private life, and no need for a concept or theory in this respect.[3] It is the invention of the art of printing and mass production of printed works that first put focus on privacy. Classic legal remedies in the penal code against libel, slander, etc. are instigated. Infringements are in written form and not quite as intensive as is the case today. It is interesting to notice that it is mainly well-known persons who can become victims of these infringements. In this period privacy is not a concept that is relevant for the common man. This observation is still valid many places today. On the other hand many data protection rules mainly concern the underprivileged part of the population. This is the case in the public sector, for example because authorities within social and employment law almost exclusively process data on these citizens. Although there are some variations it can be argued that data protection mainly protects underprivileged citizens.

As indicated, technological developments lead to new methods of infringement. Probably the most famous legal paper on privacy printed in *Harvard Law Review* (1890) is concerned with the press and in particular the use of photographs.[4] In this paper the basic rights to be let alone and to control personal information are developed. It is interesting and also somewhat disturbing that more than 100 years later these two rights still form the core of privacy and its modern form, data protection. This could indicate that legal thinking in this field has not been developed, in contrast to the radically changed environment for the private lives of citizens. The many practical issues have probably been too dominating, at least with respect to information privacy. It is tempting to conclude that the time is ripe to expand and renew the concept of privacy.

The basic idea is that people, although being part of a society, are also individuals and have a right of being their own as long as this does not undermine the collectiveness of a democratic society based on the rule of law. To a certain degree privacy can be seen as liberty and a sign of respect for each individual. From this description follows that privacy is an awkward right in the sense that it can be seen as a restriction on societal innovation. This is exactly the conflict that plays a major part in all legal policy discussions that occur with respect to data protection.

However, it is still not very clear what privacy really means. To begin with it is important to stress that it is a right of the individual in relation to others, i.e. not merely to the state but also to private corporations and ultimately to other individuals. It might be easier to define the right negatively than positively. The question is what restrictions in the individual's right to be his own can be just and acceptable? The starting point is certain, but unfortunately not very clear. Restrictions that are necessary for the common good must be accepted. In other words privacy cannot prevail when it is an obstacle to the orderly

running of a democratic society based on the rule of law. This refers both to the private and the public sector. The difficult question is what this consideration to society in practice implies. First of all it seems important to observe that the situation is dynamic, i.e. developments in society change the boundaries of privacy. Restrictions, however, must be reasonable, implying that not all societal developments can take effect. There are, for example, limitations to the extent of the personal information that it is acceptable to process in order to make a societally reasonable tax system function. This is important, as it underlines that privacy cannot be totally eroded and that there are limitations to the consideration to society.

This assumption is particularly clear when it is recalled that privacy is linked to freedom and justice. An all-dominating society contradicts these values and is accordingly not acceptable. With this background it must for each aspect of privacy to be considered on which restrictions can be accepted. This will differ from aspect to aspect, as some forms of privacy are of little societal importance. In the rest of this article focus will be on informational privacy, where the needs of modern society are very strong and where consequently it can be very difficult to uphold a reasonable sphere of privacy.

3. Modern data protection

Modern information technology has improved the possibilities of processing personal data. The computer and the networks are strong tools with respect to information. The digitalized world shares information to an extent never known before. Many benefits derive from these developments but at the same time there is little doubt that privacy, in the meaning of keeping personal information secluded and controlled, is endangered. The societal need for personal information is huge, and it has become a difficult task to maintain boundaries of privacy. These observations are not new but have been known for at least 30 years. The technological pressure has, however, become still stronger. Legislative and moral responses are difficult. The battle is by no means decided.

The legal response to these developments has been data protection legislation.[5] This started in Hessen in 1970 and the first national act came into force in Sweden in 1973. Many Western European countries have such laws today and international instruments have also been developed. OECD issued guidelines in 1981, and in the same year The Council of Europe issued its convention 108/81 that came into force in 1985. These international rules mainly try to deal with the difficult issue of transborder data flow. In 1995 the European Union issued a directive that has to be implemented by the member states before October 1998.[6] It is believed by many that this directive, outlined below in Section 5, will promote a broader international understanding and perhaps even in the long run a global convention, possibly within the scope of the WTO.

In this respect it is interesting to observe that comprehensive data protection is found only in Western Europe. Some countries like USA and Canada have laws governing the public sector, but only few rules on the private sector. Many countries have no rules at all. To some degree these differences show that privacy with respect to information is viewed divergently, and that legal culture gaps play an important role within data protection law. This aspect will be elaborated in Section 5. All in all, it is likely that data protection law will spread in the coming years, but also that this will only happen after prolonged legal policy battles due to the power and money at stake. It falls outside the scope of this article to discuss this point, and the following will focus on major principles of data protection.

4. Societal information aims

Although data protection law aims at preventing misuse of personal information, at the same time it promotes principles that can be viewed as part of privacy and justice in the information society. It is these principles that are of primary interest within the framework of this article. Probably the most important principle is transparency or openness. It must be possible for the data subject to know all the kinds of processing that his data undergo. Transparency is the tool to ensure that the information society is based on trust. As this society is extremely complex, substantive rules cannot in practice ensure sufficient legal protection. Rules of a procedural nature are more suited for this task and can easier be used by data subjects. Transparency is a tool which is not always easy to use. It consists of different elements.

First the duty of the controller to provide information. This can concern the reasons for data collection, the storage of data, the intended purposes of use and communication. To what extent such informational rights are provided depends in practice on the nature of the data and its intended use. A major issue in this connection is the costs incurred by controllers. The basic question is what price must be paid in order to use other people's data: a question to which there is only a political answer. The important assumption made here is that as a principle there is a price to pay. It is only its extent that is a political question.

Secondly there is the right of access, which has been seen as the Magna Carta of data protection. This is a right that presupposes that the data subject is active. It provides the possibility for the data subject to know which data are in the possession of different controllers. This is not an easy right to use and it is an international experience that data subjects are reluctant to do so. There are probably many different reasons for this situation. First of all, it is well-known that knowledge of a right such as this always is fairly low even though there exists a lot of information about it. This informational law is difficult to escape. Secondly each controller is independent, which means that access has to be applied for to each controller, which of course is a major obstacle. However, a situation in which access could be provided centrally would mean a possibility of central storage which for other reasons would be dangerous (the fear of Big Brother). There is no easy solution to these problems, and the right of access is not in practice the ideal instrument to ensure fair data protection. Even when this is taken into account access is still an important right for the active citizen and the possibility of access is probably also important for data discipline at many controllers. Access must still be part of data protection.

Another aspect can be participation, where the data subject has active control over data processing. This is the case where processing can only take place with the consent of the data subject. On a general level it might be assumed that it would be the normal situation when the data concern the data subject. However, this is not the case in actual legislation. There are certain cases where consent is needed and many cases where consent is sufficient. However, the main parts of data protection law are based on the assumption that consent makes a certain data processing legitimate, but also that most data processing can take place without consent. The position of the individual is not dominant in current law—an interesting observation in a field of law that directly concerns the individual. This is mainly due to the fact that it is too burdensome to acquire consent, and that this will reduce the efficiency of modern information handling. Pragmatic reasons prevent a dominant position of the individual.

On a general level this is a position that is only partly acceptable. There are certain forms of data processing that take place for clear societal reasons and here it seems reasonable that a requirement of consent would not be expedient. On the other hand there is data processing, in particular in the private sector, which is not based on such reasons, and here consent seems expedient. Whether this should actually be the case depends on how the economic system is conceived and whether the actual processing could infringe privacy. The starting point is normally that consent should not in all cases be necessary. This is, as mentioned, also assumed in most data protection legislation, and it indicates that these rules do not only take the interests of the individual into consideration. A complex mixture of interests is at work in this field of law.

From this point of view another basic informational dictum might be elaborated. This is the need for a mutual understanding of the different forms of information processing. The position of the different controllers has to be taken into account. In a modern complex society it would be too one-sided to look only at the individual. Other players must also be considered.

Let us start with public authorities, and to make things easy concentrate on the state. Let us also assume that we are in a democratic society and that there is no doubt that the state represents the majority of the population and that the minority is also respected. Such states actually do exist, and they are in particular interesting as they cannot be viewed as a threat seen from the perspective of the individual. The role of such a state is to ensure that society functions and that all citizens have acceptable living conditions. Today, clearer than previously, the state needs information to perform its tasks: information on citizens, on corporations, on non-personal issues and on international affairs. The good state is also a legal state and it is normal that the running of the state is governed by legal rules. It is not strange that processing of information is also directed by such rules. These should not give the state a free hand, but how protective should they be? Taking the purpose and character of this state into account it is not at all clear that these should be very restrictive. It must be possible for the state to handle those kinds of information which are necessary for it to play its role in society. From this point of view it follows that personal information must also be available for the state. This information must not be excessive but sufficient for the different tasks. Consequently, the rules must make it possible to prevent misuse of personal information. Even in the well-governed state it is not certain that information is processed in an acceptable way. There is an administrative urge to process all information available, and this tendency has to be curtailed by clear rules.

It is accordingly fairly clear that the state must have information, but it is also clear that this must be information that is relevant and not all other kinds of information. At the same time, as explained above, it would be too excessive to allow the state freely to process all relevant information. The legislative problem is to ensure that the state gets sufficient information and also that it does not get more. It should also be recognized that the state is not one big entity in which all information can or should be shared, but is structured in departments that have specialized tasks that determine what information is necessary. Administrative law with respect to divisions within state administration has to be respected. It is not expedient to go into any detail here.[7] The basic conclusion is that the state has a legitimate need for personal information but that this should be channelled to the different parts of the state in a precise and clear way.

Private corporations also use personal information. In many respects information is necessary in order for a corporation to function in accordance with its goals. Information on employees, competitors and not least customers (actual/potential) is essential. Such

information is a competition asset and for this reason corporations will follow a policy that provides access to as much relevant information as possible. These informational needs are basically sound and understandable. They should not be criticized as such, but there is a risk that these needs are satisfied in a way that can infringe the integrity or privacy of individuals. Some sort of legal regulation is necessary.

It is a basic feature of West-European data protection law that it is presumed that the informational relation between individual and corporation should be regulated. The position of the individual is conceived in a similar way as that of the citizen in relation to the state. This is an approach that is not recognized in many other legal systems, as it actually inserts a human rights perspective into the private sector.[8] As will be elaborated in the next section it is often assumed that the same rules must apply in the two sectors. Seen from the individual's perspective it is once again transparency and a clear and open policy that are essential requirements, together with certain specific rules placing limitations on the processing of personal data by private corporations.

Rules are actually limitations, and are for that reason not viewed kindly by corporations. This is, however, not different from the attitude to most legal interventions in the private sector. The question is whether it is an expedient attitude. Corporations are dependent on individuals as customers. They are accordingly dependent on their image and how they are seen by potential consumers. It is not sufficient to have a good product if the firm does not conform with the standards that customers deem appropriate. It is not surprising that in the information society such standards are linked to the handling of information, including personal data. This is an activity which it is difficult for the individual firm to regulate. When the state legislates and corporations have to follow the same rules the result is that processing of personal data does not become a competitive factor, but rather implies that all corporations are equal with respect to this factor. For this reason also private corporations in reality have an interest in data protection law.

5. Directive 95/46

Since 1981 the main international instrument in data protection law has been the Council of Europe convention 108/81. The purpose of the convention is the promotion of trans-border data flow on the basis of equivalent levels of protection in the different countries. For many reasons this purpose has not been fulfilled to a satisfactory extent, and as personal information has become more and more internationalized the necessity of more efficient legal instruments has become clearer. A step in this direction is taken in directive 95/46, that in general will influence European law and will strengthen the possibilities of transborder data flow (see below).

An extensive description and discussion of the many complex rules in the directive will not be given here. In the following some general features will be highlighted and a couple of interesting topics will be analysed briefly, all within the framework of the previous sections of this article. First of all the purpose of the directive should be noticed. This is stated in article 1 and falls in two parts. First the directive protects "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data". Secondly, the directive provides free flow of personal data within EU unless reasons[9] other than privacy restrict such flows. Article 1 illustrates the complex and potentially contradicting purposes behind the directive.

The consideration to fundamental rights indicates that this is a very important directive, being an attempt to create a common legal protection of individuals regardless of diverging

legal cultures within the community. On the other side, the desired free data flow makes it clear that this is a single market directive and that strong political and economic interests are at stake. The split purpose indicates that there will be many differences with respect to the interpretation of the individual rules and as to how these are to be transposed into national law—a legal policy battle which is currently being fought and which later will be replaced by disputes at the European Court of Justice. Even when these implications are taken into account it is interesting to notice that protection of personal data is conceived as a fundamental right and therefore as a consideration of importance in the legal regulation of the information society.

The basic concept of the directive is 'processing of personal data'. This is the object of regulation, and processing can simply be explained as everything that can be done with personal data (article 2b). The regulation is broad and is neutral as to which technology is applied. The directive is in this way a clear expression of the belief that data processing is essential for the well-being of individuals in the information society. Read like this it is an important statement concerning the contents of the future legal system. However, as indicated above, the directive does not provide one-sided regulation in favour of privacy. The interests in using personal data are also very much taken into consideration. Among other things this has been necessary in order to get the directive enacted.[10] Even though this had led to many modifications of the protection the directive is still the important statement described above.

As mentioned, the intention is not to provide a full description, only some examples. First, one of the basic principles, article 6 subsection 1b, states that 'personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'. This is the well-known prohibition against secondary use. It is an extremely important principle, in particular today, when all physical restraints on data processing are vanishing quickly. When it is combined with rules (articles 10 and 11) making it clear that the data subject must know the purpose, then it is clear that the principle is the basis for transparency and is against secret data processing. It furthermore places restrictions on matching of data. It is probably the most important rule in the directive, but it is open for interpretation and will often be controversial in day-to-day practice.

First of all, it must be emphasized that the principle only works if it is maintained that the purpose of collection has to be clear and precise. It must in itself have communicative value and describe boundaries surrounding the actual data processing. This is the essential point in the application of the principle and it is at this point that there often will occur a legal policy battle. If this is won it only remains to ensure that the purpose cannot be changed at a later stage. It must be maintained that this can only happen if the consent of all data subjects is given, and this will in practice mean the beginning of a new processing situation. It should be added that in practice it will not be easy to supervise that the principle is respected. Experience has shown that it is not expedient to have vast bureaucratic measures surrounding data processing. Such measures are in reality counterproductive, as they provoke opposition against the whole regulation. Although the directive (article 18) in principle states that all processings have to be notified the exceptions to this rule will be used widely, meaning that only fairly few processings will be reported formally to the supervisory authority. Data protection rules to a large degree depend on voluntary adherence.

In this voluntary situation it is mainly the data subject that has to be aware of incidents of secondary use. This is a fairly weak form of control and the task is therefore in general

to convince controllers that secondary use should not occur and that this in the long run is also in their interest. Not an easy task, but necessary.

When the directive has been implemented there will as a starting point be the same level of protection in the member states and accordingly data can flow freely within the EU (article 1). As the directive makes it possible for the member states to some extent to have different rules (see in particular article 5) and as the rules probably will be applied divergently in national practice the similar level of protection is an illusion to some degree. It will be necessary that the Commission and not least the Court are active in supervising the use of the directive to ensure that the conflicting legal cultures do not gain the upper hand.

As for third countries, the basic principle is stated in article 25 subsection 1 according to which data can be transferred insofar as "the third country in question ensures an adequate level of protection". According to subsection 2 adequacy is determined by taking all forms of regulation into consideration. There are several modifications to this rule in article 26, but in this article it is the general principle that is of interest. It can mainly be observed that the principle of adequacy seems to disregard the importance of legal culture. It is naturally assumed that the principle is practical and it is this assumption which is interesting. The question of regulation of data processing is deeply connected to fundamental conceptions of societal power distribution and the autonomy of private enterprise. Accordingly similar levels of protection are in reality very difficult to achieve, and it seems likely that major modifications will have to be recognized in practice. Seen from this perspective article 25 describes an ideal, which is well-known in the international instruments, but which has not become more realistic due to internationalization, etc. However, these assumptions do not have to lead to the conclusion that transborder data flows should not take place. Some modest similarity can often be achieved and maybe the solution can be found in intensified forms of international auditing and control. The new powers that the directive gives to the European Court of Justice is an example of such a development.

These remarks are not meant as a criticism of the directive. Article 25 is quite modest and is necessary if the directive is to have sufficient meaning. They are rather meant as a caveat against the belief in true common levels of protection. It is necessary to take legal cultures seriously and not to forget this factor in the quest for internationalization.

6. Conclusions

Privacy as a part of the broader concept of justice plays an important role in the information society. There is no doubt that the legal regulation of information linked to the individual in many ways will describe the values on which the information society is founded. The general concepts are closely linked to practical politics and their importance is not an *a priori* given fact. For these reasons it is essential to have a clear understanding of what privacy means today and how this concept is connected to the more specific concept of data protection. The assumptions reached through these analyses must then be transferred to an understanding that can be related to concrete modes of legal regulation.

In this connection it should be recognized that change occurs very often at the concrete level. This means that development of the actual rules can seem somewhat chaotic, and this observation underlines the importance of the general concepts. They can guarantee that these changes stay within a general regulatory framework that is in accordance with the values we want respected in the information society. Viewed this way it becomes clear that

the general analysis and understanding can play an important role in the framing of society and can become the basis on which the actual regulation is built.

This requires that certain demands are met. First of all it is necessary that the results of the general analysis are made known in the relevant places. The analysis must not be made in isolation or only for the chosen few. It must not be phrased in a language that is too abstract, and it should aim at being related also to actual conflicts or legal policy issues without making those the main target. It must all the time be taken into consideration how the results are communicated in the best way.

This understanding of the importance of privacy and the role of general analysis has determined the outline of this article. The aim has been to demonstrate that privacy and data protection are essential parts of justice in the modern information society. These are key aspects of a modern understanding of justice. It will always be an aim that society be just, but at the same time it must be recognized that justice is not a steady concept but is always changing, emphasizing different aspects of its multitude of elements. Today privacy in the developed world is a major aspect. Perhaps tomorrow other aspects will become more important.

That may be the case but for the time being emphasis must be laid on the current interesting aspects, the aim always being a just society with respect for privacy of the individuals that together are that society.

Peter Blume
University of Copenhagen
Copenhagen
Denmark

Notes and References

1 People is here used to mean all persons except the very young, the very old and certain handicapped persons. It is, of course, in principle a sociological concept.
2 The proposed ideas are viewed as true, but are of course in some sense the result of choice.
3 The fight against tax collectors as aspirations to maintain the authority of the family towards its members might be seen as forerunners of the idea of privacy.
4 S Warren and L Brandeis, The right to privacy, *Harvard Law Review* No. 4 (1890–91).
5 Texts of statutes and international instruments are reproduced in Wayne Madsen, *Handbook of Personal Data Protection*, Macmillan, New York, 1992.
6 Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities* L.281/31-50.
7 The question of data-sharing between public authorities is a hot legal policy issue. The Danish government prefers extensive sharing as described in *Info-society* 2000, 33–34, Ministry of Research, 1994 and also in later government plans, but the EU directive prevents such excessive data communities.
8 Such an approach is also well-known in women's law.
9 When the directive has been implemented in the member states and has come into force it will be very interesting to observe the extent to which this possibility of restricting data flow will be used by the member states and accepted by the European Court of Justice. This will provide an indication as to how strong national legal cultures remain in this field of European law.
10 From the first draft in 1990 to the final directive many amendments were made and a large part of these increased the freedom of the member states, at the same time making the regulation less exact and lowering the level of protection.