THE PROPETIZATION OF PERSONAL DATA AND IDENTITIES

J.E.J. Prins¹

Readers are reminded that this work is protected by copyright. While they are free to use the ideas expressed in it, they may not copy, distribute or publish the work or part of it, in any form, printed, electronic or otherwise, except for reasonable quoting, clearly indicating the source. Readers are permitted to make copies, electronically or printed, for personal and classroom use.

Abstract

In this article, it is suggested that, although it is all too often argued that vesting a property right in personal data is not in line with the continental, human-rights based approach to privacy, the European system definitely offers room for a property-rights model. Further analysis reveals, however, that there are doubts about whether such an approach would indeed offer the claimed prospects of achieving a higher level of personal data protection. Given developments such as ubiquitous computing, the use of personal data will increasingly occur within, and be structured by, social, economic and institutionalized settings. Thus it is suggested here that data protection mechanisms must be structured along lines of control and visibility in relation to identities, and not be based on ownership of personal data.

1. Introduction

During the past decade, many commentators and several organizations (among them the American Civil Liberties Union and the Electronic Frontier Federation²) have argued that individuals should receive fair compensation for the use of their personal data. Given the fact that protection of personal data is expensive and in short supply, whereas the collection and use of personal data is wasteful and inefficient, commentators claim that we should consider market-oriented mechanisms based on individual ownership of personal data. In the end, if markets were allowed to function more effectively, there would be less privacy invasion.³

¹ Professor of Law and Informatization, Faculty of Law, Tilburg University, The Netherlands.


Many of the arguments that have been put forward in favour of a proprietary perspective on protection mechanisms derive from American sources. There has been relatively little discussion outside the United States about whether such a perspective and approach could resolve the pressing problems of personal data protection - a fact that is not entirely surprising given the European human-rights-oriented approach to privacy protection. It is the aim of this contribution to add European perspectives to the debate. It will show that, although it is all too often argued that the creation of a property right is not in line with the human-rights-based approach to privacy, the European system appears to offer considerable room for a property rights model. However, the analysis will also show that, although vesting a property right in personal data may have some appeal, albeit for rhetorical purposes, there are doubts about whether such an approach will in our present-day society of pervasive technologies offer the claimed prospects of achieving a higher level of personal data protection.

2. Human rights and the propertization of personal data

Many different arguments have been suggested as advantages and disadvantages of vesting property rights in personal data. Aside from the commentators that have specific points of criticism, there are those who claim at a more fundamental level that such an approach does not have a future in those legal systems that value privacy as a human right. It is argued that securing privacy by means of property rights is indicative of a typical U.S. approach to the matter. In contrast, the European debate on privacy protection would take a human rights perspective on the issue: the concept of (commercial) property may not be vested in privacy because privacy is attached to individuals by virtue of their personhood, and, as such, this right cannot be waived or transferred to others (either for commercial or for other reasons). Also, human rights are conceived as closely linked to constituting and maintaining a person’s personal integrity. They are therefore seen as non-commodifiable rights.

But the human rights argument may, of course, also work the other way around: in a pure sense, the idea of human rights is all about empowerment. It could be argued that to deny individuals a property right in privacy for the reason that such an approach sits uneasily with human rights, would violate these very same rights: why should we prevent free individuals from using what means they have to strengthen their position, even if this does

---


involve being exploited by others? Denying individuals a property right would leave them less able to bargain for their interests, and thus less empowered. The question then arises what takes preference, individual autonomy or the human rights laid down in our Constitution?

The principle of individual autonomy assumes that parties enter into contracts voluntarily, guaranteeing them a considerable degree of freedom to enter into contractual obligations. This principle is also recognized in relation to constitutional law, meaning that freedom of contract even prevails when the contract sees to fundamental human rights that are accorded protection under the Constitution. Thus, under continental European law, individuals are allowed to waive the protection of their fundamental rights, albeit that the European Court of Human Rights requires that the individual who consents to waiving his fundamental rights does so in an explicit manner. When applied to personal data, the constitutional recognition of privacy thus does not prevent individuals exploiting their privacy rights by using the instrument of freedom of contract. Individuals are free to negotiate the content of agreements to best suit their needs, and to ensure the most efficient exploitation of the economic value of their personal data.

However, other legal regimes may nevertheless prevent an individual from alienating his rights in personal data. As will be known, the European Union laid down specific provisions as regards the use of personal data in its Directive 95/46/EC. An issue that thus remains to be dealt with relates to the intersection between European data protection legislation and the freedom of contracts: are contracting parties allowed to depart from the legal framework set under the European data protection Directive - and if so, to what extent? May individuals freely decide whether they want to benefit from the level of protection established by the European legislature, and does the principle of contractual freedom thus overrule the legislative balance in protecting personal data as established at the European level? Or does the European Directive limit the parties’ freedom of contract because it dictates that they should adhere to a certain minimum standard of privacy protection?

---


8 See Deweer/Belgium (ECHR 27 February 1980, A 35 §48-54); De Wilde, Ooms, Versyp/Belgium (ECHR 18 June 1971, A12 §65), available at: [http://www.echr.coe.int/Eng/judgments.htm](http://www.echr.coe.int/Eng/judgments.htm). See also, on these and other relevant rulings, R.A. Lawson and H.G. Schermers, Leading Cases of the European Court of Human Rights (Nijmegen: Ars Aequi Libri, 1997), at pp. 637-638.

9 Directive 95/46 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 individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L281/31, 1995.

10 Compare Bergkamp, who argues: ‘In other words, even if an individual wants to give up some or all of his privacy rights (e.g. to obtain a lower price for a product or service), EU law will not let him do so. The EU privacy rights cannot be waived in any matter. Consequently, any agreement pursuant to which a data subject waives some or all of his rights under the Data Protection Directive is void and unenforceable, even if the agreement otherwise meets all the validity requirements and is in the data subject’s interest’; Lucas Bergkamp, European Community Law for the New Economy (Antwerp: Intersentia, 2003), p. 123.
3. Contractual freedom, control rights and the EU Personal Data Directive

To answer the above question, we need to explore whether the specific provisions of the European Directive on personal data protection stipulate anything on their mandatory character. In the past, the European legislature has intervened several times in contractual relationships. It has found it appropriate to intervene in contractual relationships in the area of consumer protection and intellectual property rights, and thus has put in place mandatory provisions to limit the parties’ freedom of contract. Article 9(1) of the European computer program protection Directive, e.g., stipulates that ‘any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5(2) and (3) shall be null and void’. In contrast with other EU frameworks, the Directive is silent on the mandatory character of its provisions, nor does it indicate that the level of personal data protection established is of a mandatory nature. Given that in practice individuals are often ‘weaker parties’ - due to the fact that they rarely possess the sufficient information or the resources to control the use of their personal data and thus their control as a bargaining tool in exchange for certain privileges - it is somewhat surprising that the European lawmakers did not intervene in contractual relationships on the processing of personal data. Nevertheless, given that the Directive is silent on the mandatory character of the Directive’s level of protection, the logical conclusion must be that individuals are free to regulate by contract the collection, use, distribution and further processing of their personal data. Hence, contrary to what might be expected the European Directive allows parties to commercially exploit their personal data without any interference from the European data protection regime.

The conclusion that freedom of contract prevails in the area of personal data protection does not, of course, mean that the contracting parties may freely determine their relationship. Clearly, the principle of freedom of contract does not allow parties to reach a result that is most unfavourable to a weaker party. When parties contract on the processing of personal data, their relationship is affected by general principles of law (e.g. to protect weaker parties to a contract) on the basis of which a number of measures have been established to redesign the balance of power between contracting parties. Most systems of continental European law contain a vast array of legal rules that limit the stronger party’s freedom of contract. It is clear that also in the sphere of personal data, these and other measures allow the courts to interpret, supplement or correct the inequalities of bargaining power between contracting parties.

The conclusion that the EU Directive clearly facilitates a contractual approach to protecting personal data may even be taken one step further, for it could be argued that


12 Art. 8(2)(a), however, provides that member states are allowed to prohibit the processing of sensitive data even when the data subject has consented to the use of these data.

utilitarian considerations weigh heavily under the European system. As will be known, the Directive has two aims: 1) to achieve a harmonized minimum level of personal data protection in the European Union and 2) to abolish existing barriers to the flow of personal data between EU member states by allowing the free flow of personal data within the European Union. When subsequently considering the constituting principles of the Directive, one may note that in essence the regime has nothing to do with the traditional human-rights-based perspective of control and respect for the private sphere. Instead, the Directive works with a set of principles of fair personal data processing which has very little to do with fundamental interests essential to individual autonomy, dignity and freedom. The starting point of the European legal regime is that the processing of personal data is allowed in principle, provided that it is done in accordance with the stipulated principles of fairness, finality, transparency, proportionality, confidentiality and control.

Although the EU Directive favours utilitarian considerations in protecting personal data as well as allowing private arrangements regarding the level of protection, this does not imply that the framework acknowledges property interest in personal data. The European Directive is clearly not shaped from the basic perspective of an individual’s autonomy and choice regarding his personal data. Nevertheless, some instruments of control and power are included in the regime and some may thus claim that, at least in a commercial setting, a property approach may not be such a very strange phenomenon under the European regime after all. One might even argue that the European legal system on data protection appears more receptive to a property approach than the U.S. system.

However, would vesting a property right in personal data offer individuals a better instrument with which to protect their interests, thus solving present-day problems of data protection? While vesting a property right in personal data may indeed have some appeal, albeit for rhetorical purposes, the obvious question is what the consequences of such an approach would be. Is such an approach viable, and would it really offer the claimed prospects of achieving a higher level of personal data protection? I expect not.

4. The propertization and commodification of our identities

Given that, to a large extent, individuals depend on the use of their data and that personal data are the motor of our information society, a move towards a legally recognized property right in personal data will in effect not change the free public availability and exchange of these data. It may be argued that at present personal data are almost by definition part of the public domain. They are so widely available, obtainable and usable that, for practical as well as legal purposes, they seem to be inside the public domain. Would this change if property rights were vested in personal data? In theory, yes. In reality, however, personal data will continue to be widely available to organizations, companies and the public. Even if personal data were to be protected by technologies such as P3P (Platform for Privacy Preferences Project) or other technical negotiating protocols, individuals would nevertheless be willing, required or forced to make their data available for use by third parties. While titleholders of copyrighted works may to a large extent oversee the limited consequences of this decision (effects on royalties

---

14 A more detailed discussion of this argument can be found in Prins (forthcoming 2005).
obtained and ‘fame’), this is not true for individuals who decide not to sell their personal data. The axis of variation here is not that straightforward. For, in contrast to copyrighted works, decisions on access to and use of personal data may have far-reaching and sometimes unknown effects on a person’s position and abilities in everyday life. In contrast to copyrighted works, the issue of control of personal data is not so much as to whether personal data are used. Instead, it is about the specifics of the context in which the data are processed as well as the actual uses to which personal data are put. To capture the essence of this protection need, Helen Nissenbaum recently proposed the introduction of a concept called ‘contextual integrity’. This alternative concept would tie adequate protection for privacy to norms of specific contexts, ‘demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it’.15

Another way of considering the issue is by focusing not so much on the individual data, but on the effects of the present-day technologies, in particular the almost limitless surveillance capacities of new technologies, such as location-based systems, radio frequency identifiers (RFIDs) and on-line personalization instruments. In a sense, these surveillance techniques require that we shift our attention from individual sets of personal data to the statistical models, profiles and algorithms with which individuals are assigned to a particular group or ‘identity’. For these models and algorithms are privately owned, and thus unavailable for public contestation. But the interests of personal data protection seem to require that they are made known to the public and thus are part of the public domain. Let me discuss this point in some more detail.

Our behaviour in the ‘public domain’ is increasingly monitored, captured, stored, used and analysed to become privately owned knowledge about people, their habits and social identity. Indeed, the term commodification of personal data may lose its significance once we acknowledge this trend toward a commodification of identities and behaviour. It is this trend that is lacking in the present debate on privacy and property. Personal data are not used and processed anew and in isolation each time a company acquires a set of personal data. In contemporary society, ‘useful’ information and knowledge goes beyond the individual exchange of a set of personal data. In ‘giving’ his or her personal data to a certain organization, the individual does not provide these data for use in an ‘objective’ context. Today, the use and thus ‘value’ of personal data cannot be seen apart from the specifics of the context within which these data are used. Personal data processing occurs within, and is often structured by, social, economic and institutional settings.16

Thus, the question is not so much whether personal data are processed; they always are and will be, whether for legitimate or for unlawful purposes. It is an illusion to think that vesting a property right in personal data will limit the use of personal data. The problem is rather how personal data are processed, in what context, and towards what end. Therefore, the focus of the discussion should move away from entitlements to single data. What we need are instruments to enhance the visibility of and to increase our knowledge about how personal


data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes. In line with Nissenbaum’s theory of contextual integrity, ‘it is crucial to know the context - who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances’. This is a much more fundamental issue which cannot be tackled by vesting a property right in individual data. To illustrate this argument, I would like to point towards the development of ubiquitous computing environments. Ubiquitous computing will create a context-aware environment in which, by means of the coordinated use of databases, sensors, micro-devices and software agents, numerous systems scan our environment for data and serve us with particular information, based on certain notions about what is appropriate for us as unique individual persons given the particulars of daily life and context. Some thus argue that ubiquitous systems will to a large extent structure and determine our daily life, mediating our identities, social relations and social power. Not only will our homes and offices become public places, but our social identities will do so as well.

Given these and other developments in the area of ‘pervasive’ computing, the discussion about protecting personal data must become a discussion about how individuals are typified (upon what social ontology, with what goal?) and who has the instruments and power to do so. In this sense, personal data protection is not about something (i.e. personal data) that can be owned; it has everything to do with position, social ordering, roles, individual status and freedom. Therefore, privacy protection in our present-day society presumes that we have the capability to know about typifying people and to control this process. It requires the availability of instruments that enable awareness of the context in which personal data are used and to monitor the data impression that individuals are exhibiting to others. In other words, the discussion on adequate mechanisms for the protection of personal data must be a discussion on whether, and to what extent, the statistical models, profiles and algorithms that are used to generate knowledge about our individual behaviour, social and economic position as well as personal interests belong in the public domain. The commodification of our identities and behaviour does not need a property rights debate with respect to individual and isolated personal data; it requires a debate on the role of law in providing the necessary instruments to know and to control the way in which our identities are made.

18 See, e.g., the various papers presented at the workshop on Socially-Informed Design of Privacy-Enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02), Göteborg, Sweden, September 2002; available through <http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/>.
19 See Philips (2005).
21 Moreover, individuals should be able to contest that certain determinations are made, to object to certain use and to ask for alternative use.