

**Privacy aspects of addresses**  
Matthias Van hoogenbemt, Katleen Janssen

# 1 Introduction

Addresses have been around for quite some time: they provide us with the means to easily identify and locate certain places and buildings. However, there is a price to be paid for this convenience. Since we become locatable, we give up a certain piece of our privacy. For example, putting a postal address on a letter means that the letter will most likely be delivered to the right person. On the downside, we relinquish our privacy when we receive a letter: anybody who intercepts the letter will know that we live at that address.

The research in this paper deals with the privacy issues regarding addresses from a legal perspective. The European Privacy Directive<sup>1</sup> is our starting point: it helps us define what can be regarded as personal data and determine if addresses fall in its field of application.

To make the research more concrete, we will then focus on a recent Flemish initiative, called CRAB (Centraal Referentieadressenbestand). This initiative tries to implement on the level of the Flemish Community an address model and model standard that should enable a more efficient exchange of address data. The idea behind CRAB is that there should be one single authentic register for addresses to be consulted by as many (governmental) organisations as possible. To study this initiative, we will look, with our privacy related research question in mind, at the draft of the CRAB-decree, including some of its technical specifications. Some observations about the address model will be presented afterwards.

Based on the research, it is argued in the conclusion that, while addresses have to be regarded as personal data, it may no longer be reasonable to protect them as strictly as current privacy legislation seems to require.

## 2 Addresses

Historically, addresses came into existence because there was a strong need to be able to identify certain places and buildings. An address is an indirect localisation system that consists of a combination of different address components, referring to a geographical object.<sup>2</sup> Since addresses were only "ad hoc" solutions, it is not surprising that there is no uniform method for defining an address. Generally, the term "address" refers to the postal address (streetname, housenumber, town, state, postal code, country, etc.). However, in Belgium, several variations of the term are used: e.g. *the Belgian cadastre* uses a different address model to localise a certain piece of land. The *National Registry (Rijksregister)* uses an address to identify where a person is actually living and the *National Company Registry (Kruispuntbank van Ondernemingen)* has no uniform address model at all.<sup>3</sup> Given the diverse nature of an address, it is without a doubt necessary to define what, at least in this article, is meant by an address.

Such an address model has been developed by a new initiative in Flanders, called CRAB (which is short for *Central Reference Address Database* or *Centraal Referentieadressenbestand*). Art. 2 1° CRAB decree defines an address as follows: "identification of an addressable object with address components such as the name of a city, a street name, a house number and a subaddress".<sup>4</sup> In this paper these four components will constitute an address.

---

<sup>1</sup> Directive of the European Parliament and Council nr. 46/1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L*. 23 November 1995, 281, 31; from hereon "Privacy Directive"

<sup>2</sup> Ontwerp van Decreet 29 januari 2009 betreffende het Centraal Referentieadressenbestand, *Parl.St.* VI.Parl. 2008-09, nr. 2067/1, 4

<sup>3</sup> Ontwerp van Decreet 29 januari 2009 betreffende het Centraal Referentieadressenbestand, *Parl.St.* VI.Parl. 2008-09, nr. 2067/1, 4-5

<sup>4</sup> This the free translation of "identificatie van een adresseerbaar object met adrescomponenten zoals een gemeentenaam, een straatnaam, een huisnummer en een subadres"

## 3 Addresses as Personal Data

Before discussing the CRAB address model we should investigate our problem on a more theoretical level: can addresses be regarded as personal data? The European Privacy Directive is the starting point for this analysis. First, its definition of personal data is addressed. Next, the consequences of the qualification of addresses as personal data will be discussed.

### 3.1 Personal data

The definition of personal data contained in article 2 of the directive 95/46/EC<sup>5</sup> reads as follows:

'personal data' shall mean **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable person is one 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.

This definition contains four main building blocks: any information, relating to, an identified or identifiable, natural person.

#### Any information<sup>6</sup>

The term "any information" shows that the legislator wanted to design a broad concept of personal data. Personal data includes any sort of statements about a person, which can be objective (by describing certain features of that person) or subjective (by stating opinions or assessments). Furthermore, personal data is not limited to the private life of the individual. The working relations or the economic or social behaviour of the individual are personal data as well. The format of the data is of no importance either.<sup>7</sup>

#### Relating to<sup>8</sup>

It is clear that data contained in a personal file relates to an individual. Less clear is the situation where the information only indirectly refers to an individual, for instance when the data refers to an object and not to the individual. This object can belong to someone or may have an other relationship with an individual, but the object could still be traced to this person.<sup>9</sup>

Three elements can indicate that data relates to an individual. Firstly, a *content* element can single out an individual: information relates to a person when it is about that person. For example, the information stored on the chip of an electronic ID relates to the owner of the ID

---

<sup>5</sup> Directive of the European Parliament and Council nr. 46/1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L*. 23 November 1995, 281, 31; from hereon "Privacy Directive"

<sup>6</sup> Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 6; Nouwt, S., "Privacy voor doe-het-zelvers : over zelfregulering en het verwerken van persoonsgegevens via internet." in *ITeR : Nationaal programma informatietechnologie en recht*, Den Haag, SDU, 2005, 23

<sup>7</sup> The information can be alphabetical, numerical, graphical, photographic, acoustic, etc and can be kept on paper, stored in a computer, videotape, etc. (Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 7)

<sup>8</sup> Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 9; Nouwt, S., "Privacy voor doe-het-zelvers : over zelfregulering en het verwerken van persoonsgegevens via internet." in *ITeR : Nationaal programma informatietechnologie en recht*, Den Haag, SDU, 2005, 23

<sup>9</sup> For example: although the value of a house may not be regarded as personal data, but as an asset of a certain person, this information can be used to determine the extent of this person's obligation to pay taxes. In this context, the value of the house should be considered as personal data. ( Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 6)

card. Secondly, when the data is used or likely to be used for a special *purpose* concerning a specific person, this information is also regarded as personal information. For example, medical information about the parents of a patient may be used to treat that patient for a hereditary illness. Thirdly, data can relate to an individual because their use is likely to have a certain *result* by having an impact on a person's rights or interests, e.g. the analysis of the time spent on a ticket to improve the service of a help desk, may have an impact on an operator. Although the system is not intended to evaluate the performance of an operator, the system may be used for that purpose and have a considerable impact on an operator. This also means that in order to be considered as relating to an individual, it is not necessary that the data focuses on that individual.<sup>10</sup>

### **Identified or identifiable<sup>11</sup>**

For data to be considered as personal data, they have to relate to an identified or identifiable person. The name of a person is the most common direct identifier and can be the starting point to obtain a lot of information about that person, e.g. where he or she lives, their family, legal and social relations, physical appearance (when a name can be linked to a photo), etc. However, it is not necessary to have the actual name of a person. On the Web it is common to assign a unique user-id to a specific person. Because this user-id can single out a person, it has to be regarded as personal data, as "indirectly identifiable" typically means that the information relates to a unique combination of data. The unique user-id does not allow as such to identify a specific person, but combined with other identifiers gives a detailed image about one person.<sup>12</sup> Special attention should be given to the *means* to identify a person. Recital 26 of the Directive states that a person is only identifiable *taking into account all the means likely reasonable to be used either by the controller or by any other person to identify the said person*. Certain information can in the hands of one person be very easy to link to a specific person, where the same information would not help someone else at all to make a successful identification.<sup>13</sup>

### **Natural person<sup>14</sup>**

The Directive only applies to natural persons. Legal persons are in principle not covered by the Directive. However, certain rules concerning data protection might still indirectly apply. When the information about a legal person can be considered as relating to a natural person, this information is personal data.

## **3.2 Consequences**

Art. 6 of the Privacy Directive imposes certain obligations on the processor of the personal data. Essentially, the data should be processed fairly and lawfully. Because this is a broad and description, the following paragraphs<sup>15</sup> of art. 6 develop the obligations in three principles: the finality, proportionality and accuracy principle.

---

<sup>10</sup> Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 12

<sup>11</sup> Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 12; Nouwt, S., "Privacy voor doe-het-zelvers : over zelfregulering en het verwerken van persoonsgegevens via internet." in *ITeR : Nationaal programma informatietechnologie en recht*, Den Haag, SDU, 2005, 24

<sup>12</sup> For example: a criminal case appeared in the past with a lot details about the offender. Even when referring to this case years after the conviction without any identifiers, this still has to be considered as personal data, because one can easily - by going through the newspapers from that time period - establish the identity of the offender.

<sup>13</sup> For example: an IP-address may not be traceable to a specific person by the general public, but Internet Access Providers can, using reasonable means, identify the user to whom they have attributed the IP address.

<sup>14</sup> Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 21

<sup>15</sup> art.6 §1 b) to e) Privacy Directive

## Fair and lawful processing

The first paragraph imposes an obligation of transparency on the processor of personal data. The data subject should be informed what happens with his personal data. This transparency has an influence on many levels. Fair and lawful processing serves as a general principle that is further developed by the other clauses of art.6.

## Finality

Personal data "must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".<sup>16</sup> This article is commonly referred to as the finality principle and is the basis for almost every privacy related legislation.<sup>17</sup>

The purpose for obtaining the personal data should be specified and made explicit, ultimately at the moment of collection of the data. The purpose of the collection should be described as accurately as possible: a general or vague description such as "for commercial purposes" is not acceptable. The personal data should also be obtained for a legitimate purpose<sup>18</sup>. There has to be a balance between the protection of the privacy of the data subject and the interest in processing the data.<sup>19</sup> And last but not least, the further processing of the collected personal data has to be compatible with the initial purpose. As clear as this phrase may seem, it remains problematic because the extent of "further processing" is not determined. Because the collection as such is also an act of processing, the storage, consultation, dissemination, etc. all encompass acts of *further processing*. In many cases, this further processing will have a purpose incompatible with the initial purpose. However, it may still be allowed as a separate processing of the same data if the requirements (fair and lawful processing, finality, proportionality and accuracy) are met.<sup>20</sup> To assess if the purpose of a *further* processing is compatible, a number of factors can be considered: the reasonable expectations of the data subject<sup>21</sup>, the applicable legal or regulatory provisions, the nature of the personal data, the possible impact of the data, etc.<sup>22</sup>

The finality-principle should be distinguished from the fair procurement of personal data: even if the personal data was procured for a specific purpose, the data may still be obtained in an unfair way.<sup>23</sup>

## Proportionality

A first set of proportionality requirements is that the collected personal data should be "adequate, relevant and not excessive" to attain the predetermined purpose.<sup>24</sup> *Adequate* means that the collected data should be sufficient to achieve the intended purpose. This requirement should be assessed from the data subject's point of view: when certain data enable the processor to achieve the predetermined goal, these data are adequate, even though this may not be the most efficient way for the processor.<sup>25</sup> *Relevant* should always be assessed *in concreto*: for each processing act, the exact purpose should be determined. *Not excessive*

---

<sup>16</sup> art.6 §1 b) Privacy Directive

<sup>17</sup> De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001, 116

<sup>18</sup> also called "justified purpose"

<sup>19</sup> De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001, 118

<sup>20</sup> The purpose of the *further processing* should be specified and made explicit and the data subject should be notified; De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001, 121

<sup>21</sup> The reasonable expectations can only be assessed on a case by case basis: the compatibility will be determined by considering if the data subject could reasonably expect that his personal data would be processed for an other purpose than the initial one. (De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001, 121-122)

<sup>22</sup> De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001, 120-122

<sup>23</sup> De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001, 116

<sup>24</sup> art.6 §1 c) Privacy Directive

<sup>25</sup> De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001, 124

means that the unrestrained collection of data that might be useful in the future is not allowed. A second proportionality requirement is that personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.<sup>26</sup> This requirement demands that for every collection a reasonable, and thus proportional storage period is determined. In other words, the proportionality principle prohibits the indefinite storage of personal data.

### Accuracy

Art.6 d) Privacy Directive is very clear: data should be accurate and when they are not, they should be corrected. The controller<sup>27</sup> should guarantee that this quality requirement is met.

## 3.3 Application to addresses

It is clear that an address is information that relates to an identifiable person. An address can easily be tied to a certain geographical location, e.g. a building or a piece of land. Whether a person lives at that geographical spot or just owns the piece of land, it is still possible to link the address to that person. Since a company may be established at that address, the address could possibly not be regarded as personal data. However, when the address refers to a natural person, there is no doubt that an address falls in the field of application. Therefore, the processing of addresses should respect the principles as set forth in art.6 of the Privacy Directive.

## 4 CRAB

Now that the consequences of the categorisation of an address as personal data on a theoretical level have been determined, the CRAB-address model should be studied more closely. During the drafting of the decree that will implement a legal basis for this address model, the Belgian Privacy Commission was consulted and answered some fundamental questions regarding privacy issues of addresses. Therefore, the CRAB-address model is a good case study to make our findings more concrete.

Accurate addresses are necessary for a government to operate in an efficient way. Because there were a lot of discrepancies between the existing address databases, the Flemish government deemed it necessary to create one central information structure, that, in time will be the sole source for address information. Hence the CRAB-initiative was founded.<sup>28</sup>

One problem, if not the most important problem, was the large number of existing different address models, which made consolidation and interoperability impossible. The CRAB-address standard proposes a model of address components that can function as a basis for other address based applications. An address modelled after the CRAB-standard at least contains the following components: street name(code), house number, apartment number and city(code).<sup>29</sup> On top of this a CRAB-address can contain information about the geographical location of the address, history of the address and other metadata.

---

<sup>26</sup> art.6 §1 e) Privacy Directive

<sup>27</sup> Art.2 d) Privacy Directive defines a controller as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

<sup>28</sup> Ontwerp van Decreet 29 januari 2009 betreffende het Centraal Referentieadressenbestand, *Parl.St.* VI.Parl. 2008-09, nr. 2067/1, 3

<sup>29</sup> AGIV, *Aanbeveling betreffende de uitwisseling van adresgegevens*, 16 mei 2008, <http://www.agive.be>, 2

## 4.1 CRAB address model

### Street name

The object *Street name* in the CRAB-address model contains the following elements that can be relevant from a privacy perspective: the name of the street, a unique identifier of that streetname and a unique identifier of the city where this street is situated. These elements as such do not permit the identification of a person, but the combination of the three elements might enable one to single out an individual. However, this will only be the case when dealing with remote and uninhabited areas where only one person lives in a certain street. Only in that case that person can be individualised by using the information provided by the *Street name*-object. Since this situation is highly unlikely to occur, in general, the *Street name*-object should not be regarded as personal data.

### House number

The *House number*-object as such is not that relevant because it does not reveal the identity of an individual. However, the *House number*-object is part of a CRAB-address that also contains the *Street name*-object. The combination of these two objects is sufficient to pinpoint a location that can be linked to an individual. Furthermore, the geographical location of the address is also stored in this object of the address model. It is clear that the *House number* together with the *Street name* should be considered as personal data.

### Dissemination

The draft CRAB-decree<sup>30</sup> states in article 19 how the information from the CRAB-database has to be disseminated to the public. First of all, a distinction is made between *public information* (street, house number, city, postal code and a unique geographical identifier) and *identifiers*. Although the Belgian *Privacy Commission*<sup>31</sup> clearly states that the *public information* still is personal information (using the address, it is possible to identify the owner of a certain piece of land), the commission is not opposed to the dissemination of this information. It deemed the impact on the privacy of an individual to be at an acceptable level, so there is no convincing argument against the dissemination. However, the consultation of the other data as well as the identifiers<sup>32</sup> needs a preceding authorisation of the *Flemish Supervision Commission (Vlaamse Toezichtcommissie)*. This *Supervision Commission* investigates and decides on a case by case basis if a specific consultation is in line with the privacy regulations.

### History

As was mentioned above, article 6 of the Privacy Directive states that personal data may only be kept for the time needed to achieve the intended purpose. However, the *CRAB-decree* states in the explanatory memorandum<sup>33</sup> that the data contained in the CRAB-database should never be deleted. Practical reasons are given as a justification for this non-archiving policy. In order to present a user with a list of records that should be added or deleted, it is necessary to keep the historical details of every address. The Privacy Commission strongly advised against this policy, since it found this policy to be offending the privacy legislation principles.

---

<sup>30</sup> A *decree* in Belgium is a law passed by a regional parliament, in this case the Flemish parliament. At the time of publication the *decree* was approved by the parliament but has not been published yet.

<sup>31</sup> *Commissie voor de bescherming van de persoonlijk levenssfeer* (<http://www.privacycommission.be/>)

<sup>32</sup> This will be a unique code for every address so that it can easily be identified and linked

<sup>33</sup> Ontwerp van Decreet 29 januari 2009 betreffende het Centraal Referentieadressenbestand, *Parl.St.* VI.Parl. 2008-09, nr. 2067/1, 7

## 4.2 Observations

### Advantages of CRAB

It is clear that the *CRAB*-database will be beneficial for the government. First, it will diminish the costs for the institutions who used to keep their own address databases. In the future, these institutions can and may have to rely upon the *CRAB*-database to keep their data up to date. Furthermore, these institutions will no longer bear the cost for the collection, verification, linking and maintaining of address information. Second, the accuracy of governmental databases should improve since the data would not need to be corrected any longer

### Linking and Analysis

Since *CRAB* will serve as a standard, the linking of different databases should become easier. Because *CRAB* will implement a standard way of encoding addresses, it can serve as a go-between for different databases. Especially when representing address data in a cartographic way, *CRAB* can become a very powerful tool for analysis. However, as tempting and progressive these linking and analysis possibilities may seem, the privacy consequences are considerable.

An excellent example is the combination of crime and address databases. The cartographic representation of crime data could help the police to link certain crimes together, to patrol more efficiently, to fight organised crime, etc. However, even malefactors have the right 'to be left alone'. A recent Belgian example illustrates this downside. In attempt to aid in the battle against child-pornography, a website was created by an anxious citizen listing information<sup>34</sup> about sex offenders. In specific instances the location was nearly accurate enough to pinpoint a particular individual. The Belgian *Privacy Commission* advised against this privacy violation. Even *Child Focus*, the Belgian branch of the *European Center for Missing and Sexually Exploited Children*, protested against this dissemination because it could also lead to an invasion of the privacy of the victims. After a few days the site was taken down.

Another possibility is to establish a link between *CRAB* and the immigration database. This could help the immigration office to develop a well-reasoned city wide or even country wide immigration policy. However, history teaches us that it may not be a good idea to make ethnical groups identifiable or locatable.

Next, charting occurrences of diseases could help identify certain illnesses caused by the environment. However, insurance companies might be unwilling to insure, or may charge a higher fee for life insurance to people living in these contaminated areas. A final example is traffic accidents. A geographical representation may help to identify dangerous crossings, but again this information may be abused by insurance companies.

## 5 Addresses: a privacy issue?

Before coming to our conclusion on whether the processing of addresses could cause privacy concerns, the question is placed in the broader context of the debate on privacy.

### Privacy in general

Nobody will contest that personal data are indeed subject to privacy regulation.<sup>35</sup> Even better, data protection has to be regarded as one of the cornerstones of our privacy protection. But what exactly are we trying to protect? In short, what exactly is privacy? Unfortunately, answering this question in detail would go beyond the scope of this article, but still some

---

<sup>34</sup> Information such as names, addresses, photos, etc.

<sup>35</sup> Gutwirth, S., *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Den Haag, Rathenau instituut, 1998, 27

general remarks can be made.

SOLOVE states that these days, "privacy is a concept in disarray".<sup>36</sup> Nobody is capable of providing a coherent view on the matter. However, it may be that such a coherent or single view is simply not possible or even desirable. Privacy is an inherently relative concept, determined by time, place, history, culture, etc. Furthermore, privacy spans a lot of different subjects: sexuality, health, bodily integrity, self-determination, personality, relations, ideology, etc.<sup>37</sup>

However, this complexity should not prevent us from trying to chart the problem. Privacy problems we now experience can be linked to the *information society* that started around the 1960s.<sup>38</sup> Given the rate at which technology evolves<sup>39</sup> we are no longer held back by practical limitations, resulting in an almost unlimited processing power. The possibilities for combining data are infinite, so the consequences of well-intended information gathering may be enormous.<sup>40</sup> Therefore, boundaries are necessary: data collection and processing should be limited to a safe level. However, where do we place that limit?

One way to approach the privacy question is the idea of *information control*.<sup>41</sup> The collection, classification, processing and transmission of personal information is one of our main privacy concerns. An individual should be free to determine who knows what about him. According to Gutwirth, the processing of personal data from a particular person gives power over that person: someone will always act differently when he knows he is being watched.<sup>42</sup> Therefore an individual should be able to control which information he makes public and how much is known about him by the public.<sup>43</sup> However, is it still feasible to claim total control over our personal information? A lot of personal information is already publicly available. How can one claim privacy on something that is already known to the public? Should we demand legislation to protect us? Yet, law alone may not be sufficient to prevent unwanted intrusion into our privacy, because it is not always the most efficient protection method.

However, a more nuanced view should be taken on the issue. Although the processing of personal data has taken massive proportions, a citizen should still have control over what is known about him. Otherwise, every individual becomes completely transparent and thus controllable.<sup>44</sup> However, the battles should be picked wisely: we should try to preserve privacy in those areas where it is still possible.

### **The processing of addresses as a privacy issue?**

The CRAB-initiative and the privacy problems surrounding it raise some very fundamental questions about the relationship between addresses and privacy. Although an address is clearly traceable to a certain individual, one can pose the question if there should be any privacy concerns purely with regard to addresses.<sup>45</sup> In our information society, addresses have become

---

<sup>36</sup> Solove, D.J., *Understanding privacy*, Cambridge (Mass.), Harvard university press, 2008, 1

<sup>37</sup> Gutwirth, S., *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Den Haag, Rathenau instituut, 1998, 15-26;

Solove, D.J., *Understanding privacy*, Cambridge (Mass.), Harvard university press, 2008, 4; De Hert, P., *Privacy en persoonsgegevens.*, Brussel, Politeia, 2004, 14/31

<sup>38</sup> Solove, D.J., *Understanding privacy*, Cambridge (Mass.), Harvard university press, 2008, 4

<sup>39</sup> Moore's law illustrates this by stating that the amount of transistors on a regular computer chip doubles every two years

<sup>40</sup> Gutwirth, S., *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Den Haag, Rathenau instituut, 1998, 28

<sup>41</sup> Gutwirth, S., *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Den Haag, Rathenau instituut, 1998, 26

<sup>42</sup> Gutwirth, S., *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Den Haag, Rathenau instituut, 1998, 27

<sup>43</sup> On the other hand, these days a privacy paradox seems to arise: although most people are aware of and are concerned about their privacy, some do not hesitate to share intimate thoughts on for example social networking websites (Solove, D.J., *Understanding privacy*, Cambridge (Mass.), Harvard university press, 2008, 5)

<sup>44</sup> Gutwirth, S., *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Den Haag, Rathenau instituut, 1998, 29

<sup>45</sup> For example, "the white pages" (telephone directory for natural persons) allow to localise a specific natural person using two identifiers, i.e. the surname and the name of the city. This geographical information is necessary

basic information, so that one might argue that privacy on an address does not exist anymore. As addresses as such are already widely spread, so there is no point in trying to rigidly apply privacy protection. Even if we would like to give addresses the same privacy protection as other personal data, it is no longer feasible. *De facto*, privacy does not extend to addresses as such anymore. Furthermore, although we might not be able any longer to control who can look up our address, the privacy implications are minimal.<sup>46</sup> The public knowledge that we live at a specific address will not harm us that much.

However, privacy legislation should fully apply on the link between the address and other data. For instance, the average house value of our neighbourhood might be very interesting information for Treasury in assessing taxation levels and revenues. Such combinations of databases should be addressed very carefully. A criminal should still have the right not to be included on a website, a patient should still have the right to not participate in a geographical survey concerning the disease he contracted, etc. These examples illustrate the numerous possibilities the linking of databases provides, but also show the downside: the privacy of the people involved in the analysis can be violated. Techniques that reduce the privacy impact of storing personal data should be employed as much as possible (anonymisation, access control, etc.)

The greatest challenge will be making the distinction between processing of addresses as such and linking with other datasets. A clear definition of an address by defining its constituting elements can provide inspiration to draw a distinct border. In Belgium, the definition of an address provided by the CRAB-decree may serve as a criterion but CRAB is an initiative that still has to prove itself.

## 6 Conclusion

Since an address constitutes information that can indirectly identify a natural person under the Privacy Directive, addresses should be regarded as personal data and privacy legislation should be applied. However, given the public nature of an address, it is not feasible to apply the requirements of privacy legislation to their fullest extent. A more pragmatic approach would be to provide limited protection to an address as such, but guard rigorously the privacy implications when addresses are being linked to other data. However, since privacy is highly subjective and driven by social consensus, only time will determine the degree of privacy that will be attributed to addresses...

---

to be able to make a distinction between people sharing the same surname and to assure that we found the right person. Although this may strike as trivial, being locatable given those two broad personal data is a considerable violation of one's privacy. However, despite the fact that we cherish our own privacy, most people like to be reachable in this way.

<sup>46</sup> Ontwerp van Decreet 29 januari 2009 betreffende het Centraal Referentieadressenbestand, *Parl.St.* VI.Parl. 2008-09, nr. 2067/1, 79

## References

- [1] Directive of the European Parliament and Council nr. 46/1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Pb. L.* 23 November 1995, 281, 31.
- [2] Article 29 Data protection working party, *Opinion 4/2007 on the concept of personal data*, 20th June 2007, 01248/07/EN, WP 136.
- [3] Ontwerp van Decreet 29 januari 2009 betreffende het Centraal Referentieadressenbestand, *Parl.St.* VI.Parl. 2008-09, nr. 2067/1.
- [4] AGIV, *Aanbeveling betreffende de uitwisseling van adresgegevens*, 16 mei 2008, <http://www.agive.be>.
- [5] De Bot, D., *Verwerking van persoonsgegevens*, Kluwer, Antwerpen, 2001
- [6] De Hert, P., *Privacy en persoonsgegevens.*, Politeia, Brussel, 2004.
- [7] Solove, D.J., *Understanding privacy*, Cambridge (Mass.), Harvard university press, 2008.
- [8] Gutwirth, S., *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Den Haag, Rathenau instituut, 1998.
- [9] Nouwt, S., "Privacy voor doe-het-zelvers : over zelfregulering en het verwerken van persoonsgegevens via internet." in *ITeR : Nationaal programma informatietechnologie en recht*, Den Haag, SDU, 2005.
- [10] Beresford, A.R., "Chapter 13. Privacy Issues in Geographic Information Technologies" in *Frontiers of Geographic Information Technology*, 2006.
- [11] Van Loenen, B. and de Jong, J., "SDIs and Privacy: Conflicting Interests of the Spatially Enabled Society", Chapter 21, In A. Rajabifard (ed.), *Towards a Spatially Enabled Society*, University of Melbourne, 2007, pp. 271-284.