Ethics Inf Technol (2010) 12:87–95
DOI 10.1007/s10676-009-9212-z

ORIGINAL PAPER

Inaccuracy as a privacy-enhancing tool

Gloria González Fuster

Published online: 29 October 2009

Abstract The accuracy principle is one of the key standards of informational privacy. It epitomises the obligation for those processing personal data to keep their records accurate and up-to-date, with the aim of protecting individuals from unfair decisions. Currently, however, different practices being put in place in order to enhance the protection of individuals appear to deliberately rely on the use of 'inaccurate' personal information. This article explores such practices and tries to assess their potential for privacy protection, giving particular attention to their legal implications and to related ethical issues. Ultimately, it suggests that the use of 'inaccurate' data can potentially play a useful role to preserve the informational autonomy of the individual, and that any understandings of privacy or personal data protection that would tend to unduly limit such potential should be critically questioned.

Keywords Data protection · Informational privacy · Informational self-determination · Privacy · Surveillance

Abbreviations

ECHR	European convention of human rights and fundamental freedoms
EU	European Union
OECD	Organization for economic co-operation and development
PETS	Privacy enhancing technologies
US	United States

G. G. Fuster (✉)
Institute for European Studies (IES), Research Group on Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB), Pleinlaan 15, 5th floor, 1050 Brussel, Belgium
e-mail: Gloria.Gonzalez.Fuster@vub.ac.be

Introduction

The principle of accuracy has a longstanding tradition, as it has been recognized as a fundamental feature of informational privacy in both sides of the Atlantic for almost four decades. The objective of this article is certainly not to diminish its importance. The aim, on the contrary, is simply to contrast expansive understandings of such a principle in the light of current practices that support, or even willingly encourage, the use of 'inaccurate' personal data. Moreover, it is suggested that there might actually be an important role to play for such 'inaccurate' data in the preservation of the informational autonomy of individuals.

The article is organised as follows: firstly, a very brief introduction to the accuracy principle is proposed. Secondly, a series of practices relying on the use of 'inaccurate' personal data are discussed. Thirdly, an attempt is made to review these practices from a legal and ethical perspective.

The importance of data being accurate

The principle of accuracy is one of the original principles of informational privacy. In a nutshell, it can be described as the duty imposed on those processing the personal data of others to ensure that the data processed is as accurate and as up-to-date as necessary. Behind such a principle stands the idea that the storing and the processing of inaccurate data can lead to unfair decisions being taken.

1970s databanks and diligent record-keeping

The origins of the accuracy principle can be traced back to the 1970s, when the so-called 'fair information practices'

were first developed in the United States (US). The advent of information technology and, in particular, the surveillance potential of computer systems had prompted demands for new rules and principles governing the handling of personal information. 'Fair information practices' can notably be found in the organization for economic co-operation and development (OECD) guidelines on the protection of privacy and transborder flows of personal data,[1] adopted by the OECD members in 1980. By virtue of one of the 'basic principles of national application' that these Guidelines established,[2] namely the 'data quality principle', "[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date".

In Europe, 'fair information practices' received support through the adoption in 1981, by the Council of Europe, of the convention for the protection of individuals with regards to the automatic processing of personal data, known as convention 108.[3] Convention 108 lists its own series of 'basic principles for data protection',[4] which are very similar to those of the OECD Guidelines and, unsurprisingly, include a principle on 'quality of data', establishing that "personal data undergoing automatic processing shall be (…) accurate and, where necessary, kept up to date".[5]

The rationale behind these provisions needs to be put in the context of the computing practices of the time. The explanatory report to Convention 108[6] explicitly links the content of its article on accuracy to the fulfilment of two legal standards: one related to the fact that information should be correct, relevant and not excessive in relation to its purpose, and one regarding the correctness of the use of such information.[7] The report also makes an explicit reference to a Council of Europe's Resolution of 1973[8] which identified accuracy[9] as the first principle to apply to personal information stored in electronic databanks, justifying its importance with the notion that "computerised information can give a semblance of special reliability" and that "mistakes may cause serious damage, because of the intensive use that can be made of the data".[10]

Accuracy was, at the time, clearly configured as an obligation of diligence for those handling the data, aimed at compensating for the unprecedented power that computing placed in their hands. It was unquestionably a duty falling on them, and not on the individuals to whom the data related. Additionally, the 'accuracy' of data was systematically presented as a relative accuracy: data are required to be accurate to the extent necessary for the purpose of the processing, but not more accurate than that.

The fundamental right to have data rectified

The development of informational privacy in the European Union (EU) eventually led to the creation of a specific fundamental right to the protection of personal data. This right obtained recognition at the highest level in 2000, when it was included in the European Charter of Fundamental Rights[11] as an autonomous right, independent from the right to privacy.[12] The EU fundamental right to the protection of personal data is characterised by its positive,[13] assertive features, which help in differentiating it from the right to privacy. If the right to privacy can be

[1] Organization for economic co-operation and development (OECD) (1980).

[2] See part two of the OECD guidelines. The principles on which these practices are based are: the 'collection limitation principle', the 'data quality principle', the 'purpose specification principle', the 'use limitation principle', the 'security safeguards principle', the 'openness principle', the 'individual participation principle', and the 'accountability principle'.

[3] Council of Europe (1981).

[4] In Chapter II. The principles listed are: 'duties of the parties' (Article 4), 'quality of data' (Article 5), 'special categories of data' (Article 6), 'data security' (Article 7) and 'additional safeguards' (Article 8).

[5] Article 5 in its entirety reads as follows: "Personal data undergoing automatic processing shall be:

(a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored".

[6] Council of Europe (1981).

[7] The relevance granted to such legal standards rests on the idea that those responsible for processing personal data should make sure that the processing does not *"lead to a weakening of the position of the persons on whom data are stored";* for this reason, *"they should maintain the good quality of the information in their care"*. The explanatory report clarifies that the provisions of Article 5 are largely identical to the corresponding principles laid down in two previous Council of Europe's (1974).

[8] Council of Europe (1973).

[9] Referred to as the principle of 'quality of the information stored' (according to which personal information should *"be accurate and should be kept up to date")*. The Resolution set out also that every care "*should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way"* (Resolution 73(22), p. 2).

[10] *Ibidem*, p. 7. A principle of correction and erasing of the information is defined as a corollary principle, and is clearly described as an obligation incumbent on *"those responsible for data banks"* (*ibidem*, p. 9).

[11] Charter of Fundamental Rights of the European Union (2000, 1–22).

[12] The right to the protection of personal data is established by Article 8, whereas the right to privacy is established by Article 7. See: Bygrave (2002a), Hustinx (2005, pp. 62–65).

[13] Poullet and Dinant (2004, p. 23).

compared to a shield, the right to data protection is more like a weapon in the hands of individual.[14] It grants a series of concrete, subjective rights that can be put into action by individuals to compensate for imbalances of informational power.[15]

One of the subjective rights to be found at the very core of the right to the protection of personal data is the right to require the rectification of inaccurate data. Convention 108 of the Council of Europe established that right as an 'additional safeguard' for the individual.[16] The 2000 EU Charter explicitly recognises it as part of the fundamental right to the protection of personal data.[17] Moreover, the right to have data rectified appears regularly in different EU legal instruments: it can be found, for instance, in Directive 95/46/EC[18]; in the 1990 Schengen Convention[19]; the Europol Convention[20]; or in the context of Eurojust.[21] Even if the right to have inaccurate personal data rectified appears unknown to a certain part of the European population,[22] its very existence and wide legal recognition echo the importance granted to the accuracy principle as a mechanism to encourage compliance with lawfulness requirements.

There is no doubt that the principle of accuracy as a duty for those processing the personal data of others is still fully relevant. Since the 1970s, however, information exchanges have been profoundly transformed worldwide. In the context of current practices, the use of inaccurate data for privacy-enhancing purposes has emerged.

Current privacy-enhancing uses of inaccurate data

The legal approach is only one of the strategies that can be adopted to support privacy. Another extremely important approach refers to the use of technology. Moreover, individuals can also be directly engaged in the preservation of privacy through self-protective practices. In these fields, the deliberate use of inaccurate data has already come to play a relevant role. Misrepresentation, partial truths, or the creation of 'clouds of inaccuracy' are some of the techniques currently being deployed in the growing but understudied field of responses to surveillance.[23]

Self-protection through noise and false information

The discussion of technology as a key element in the protection of privacy has become increasingly popular in the last years. In particular, discussions have developed around buzzwords such as 'privacy enhancing technologies' (PETs)[24] or 'privacy-by-design', and special consideration has been given to how particular technologies and

[14] Privacy and data protection have notably been conceptualised as divergent forces in terms of opacity and transparency (De Hert and Gutwirth 2006). Critical assessments have highlighted the potential of data protection laws as a legitimizing tool for potentially privacy infringing interferences (William and Chiasson 2005, p. 271).

[15] See also: Gutwirth (2002).

[16] Article 8(c) of Convention 108 foresees, under the title 'Additional safeguards for the data subject', that any person shall be enabled to "*obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles*". Note, however, that the Convention's provisions do not elucidate whether individuals might exercise their right to correct during the collection of the data or when the automatic processing has begun (Yuste 2001).

[17] Article 8.2 establishes in this sense that "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

[18] Directive 95/46/EC (1995, 31–50); see also: Directive 2002/58/EC (2002, 37–47). Section V of the data protection directive deals with 'the data subject's right of access of data', and consists of a single Article (Article 12), on the 'right of access'. By virtue of said Article, every data subject (defined as the natural person to whom relates the personal data in Article 2(a) of the same Directive 95/46/EC) is granted the right to obtain from those processing personal data "*as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data*". This is complemented by the obligation to notify to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out unless this proves impossible or involves a disproportionate effort (Article 12(c) of Directive 95/46/EC).

[19] Convention implementing the Schengen Agreement (1990); on account of its Article 110: "*Any person may have factually inaccurate data relating to them corrected* (…)".

[20] Council Act (1995). It also foresees the obligation to keep data accurate [see Article 20(1)] and allows for any person to request rectification or deletion [Article 20(4)].

[21] Council Decision (2002, 1–13). Eurojust actually explicitly grants the right to require the 'correction' of personal data not only to any person concerned (see Article 20), but also but also to Member State's competent authorities, national members and national correspondents [see Article 20(3)].

[22] According to a recent EU-wide survey, 13% of respondents declared that it was not true that they had the right to correct or remove data which is inaccurate or has been obtained unlawfully, and 10% did not answer the question (Gallup Organization 2008, p. 26).

[23] As stressed by Marx in 2003 when he proposed a categorisation of what he describes as 'behavioural techniques of neutralization intended to subvert the collection of personal information', classified as: discovery moves, avoidance moves, piggy backing moves, switching moves, distorting moves, blocking moves, masking moves, breaking moves, refusal moves, cooperative moves and counter-surveillance moves [Marx (2003), http://web.mit.edu/gtmarx/www/tack.html]. In this sense, it has been stated that "creative responses to surveillance proliferate along with awareness that surveillance affects our everyday lives" (Lyon 2007, p. 167).

[24] See, notably: Bygrave (2002b), European Commission (2007).

techniques can contribute to ensure, and even reinforce, the privacy of individuals. Modern privacy-preserving and privacy-enhancing techniques can rely on the use of inaccurate data at different levels or stages. For example, so-called 'perturbation techniques' aim at increasing the confidentiality of information by 'perturbing' data with random noise.[25] If noise can facilitate the undetectability of data,[26] misinformation and disinformation can contribute to its unlinkability,[27] the production of 'dummy traffic' being a particular mechanism to implement this kind of strategy.[28]

The use of inaccurate data can also be incorporated in the design of applications or interfaces. An interesting illustration can be found, for instance, in the service recently launched by Google to support social networking using location-related data, called Latitude.[29] The service is designed to allow people to constantly share information about their location with other persons, providing data through their mobile phones or computers. Understandably, the service has raised many privacy concerns. What is worthwhile noting here are two of the features that the company has incorporated into the service in order to try to mitigate privacy concerns.

First, the application allows users to share with certain individuals data which is less precise than the data shared with others: instead of providing them with their exact location, users can chose to communicate to certain individuals only a 'city' location. Managing the degree of precision[30] of data is thus presented as a privacy-preserving mechanism. Second, even if the 'standard mode' for the participants is to automatically provide data about their location via their devices, the users can change this mode and decide either to completely hide their location or 'to set it manually'. By setting the location manually to a location not corresponding to the real one, users can protect location-related data they perceive as too private to be shared, without having to cope with the disadvantages of explicitly disengaging from the system.

The two features described might not by themselves render the whole service as privacy-enhancing as desirable. What is relevant here is that they rely on the assumption that individuals are in principle not against the idea of being, at least to a certain extent, not fully loyal to facts, especially if this helps them protect their privacy. Admittedly, individuals do sometimes prefer to provide inaccurate information about themselves. The aim of this article is not to discuss how often do people lie, but to emphasise that they sometimes consciously do so for the (arguably legitimate) purpose of privacy protection.

A very common scenario for the disclosure of inaccurate personal data occurs when the individual is confronted with apparently disproportionate demands of personal information. This is particularly frequent in on-line environments. In order to access a service, the individual can be invited to, or, more worryingly, obliged to, provide data that seems to be unnecessary for the purposes in question. Often, such extravagant demands will be not only annoying, but also plainly illegal, as requiring unnecessary data is itself contrary to many international and national privacy provisions. Forced to choose between renouncing the service by not disclosing unnecessary personal data, or accepting the transaction by disclosing such data, the individual might decide to subvert the whole trade-off, and opt for a third possibility: provide *some* information, namely inaccurate data, with the objective of accessing to the service while protecting data considered worth preserving. The disclosure of inaccurate data can thus be used as a tool facilitating the modulation of consent to the disclosure of data.

A specific field in which inaccurate data plays an important role is social networking. Social networking applications and sites are often perceived as enabling a global erosion of privacy and data protection, as large quantities of data are provided by those participating in such networks. This perception, however, needs to be nuanced by a careful consideration of the quality of the data provided by the users. Although empirical research is still not fully developed, studies in the field tend to confirm that at least part of the personal data provided by users is false. A recent study on US teenagers revealed that 46% of respondents declared to have provided false information on their online profiles.[31] Users appear to have a clear notion, or at least some notion, of the correlation between the accuracy of the data provided and the identifiable nature of such data.[32] Internet users in general seem to discriminate between different categories of data, and appear to be inclined to provide inaccurate data for certain types of data considered worth protection.[33] Inaccurate data in this

[25] See, for instance: Kargupta et al. (2003), Liu et al. (2008).

[26] Pfitzmann and Hansen (2008, p. 15).

[27] *Ibidem,* p. 12.

[28] *Ibidem,* p. 19.

[29] More information can be found here: www.google.com/latitude/intro.html.

[30] And thus of accuracy, if the latter is defined as the quality or state of being correct or precise.

[31] Lenhart and Madden (2007)

[32] More than half of the respondents who declared that 'all' or 'most' of the information on their profile was fake said that, in their view, it would be difficult to determine who they were from their profile (*ibidem*, p. 26).

[33] According to another study, only 65% of the total general public always or often use their real names when registering at a website, even if 80% would use their real e-mail addresses and 81% their real ages [Online Computer Library Center, Inc. (OCLC) (2007, p. 15)].

context appears as an element facilitating modulations of user choice between exposure and shielding.

Creative approaches to profiling

The uses of inaccurate personal data are not limited to protective, disguising or covering strategies. The provision of inaccurate data can also play a function in relation to profiling and predictive data mining practices,[34] where large quantities of data are processed, permitting the identification of a series of patterns. These patterns are later to be used to allow for certain decisions to be taken, by being applied to individuals that appear to match a relevant pattern. Predictive data mining is currently being implemented in a variety of fields.[35]

A series of Web 2.0 applications are based on the use of data mining and profiling practices to provide the users services allegedly better fitting their preferences. The 'accuracy' of the results obtained through data mining, however, is not always proportional to the 'accuracy' of the data mined. What is proposed as the 'right' content for the profiled user is not always the 'right' content in the eyes of the user,[36] even when the data processed appears to be fully accurate. Arguably, it might be the case that creatively manipulating the data used for profiling will increase the satisfaction obtained with using the service.

A concrete example of an application allowing this type of creative interactions is the service for music recommendations Last.fm.[37] This application tracks the listening habits of its users in order to provide music recommendations supposed to match their personal tastes, as well as group recommendations supposedly corresponding to the preferences of certain groups of users. In its 'normal' mode, the application will automatically register all the pieces of music that the user listens to, and mine this data to infer information both about the personal tastes of the listener and on general listening practices. The user, however, is given the possibility of reviewing the pieces of music automatically listed, and of altering them. Through this manipulation, users can try to contribute to the rightfulness of the knowledge inferred by the system, and, for instance, avoid that the music listened to in a special, unusual circumstance is processed to produce generally non-fitting recommendations. By altering the (accurate) information about them, users can interact more freely with the system and, in principle, obtain better benefits from it.

The potential importance of the use of inaccurate data to enhance the role of individuals in the construction of knowledge about them, and about society in general, through data mining and profiling techniques, needs to be placed in the context of current discussions on such techniques. As the construction of knowledge is increasingly reliant on the external generation of conclusions based on not always clear inferences, looking for means to allow for meaningful individual participation becomes a priority.[38] Playing with the degree of accuracy of the data feeding the process might be a relevant tool to give to individuals a role to play in their self-representation and self-definition, as well as in the definition of categories affecting the others.

Assessing the potential of inaccuracy

Having described some privacy-enhancing practices deliberately relying on inaccuracy and their different functions, it is necessary to consider such practices both from the legal and ethical perspectives.

Legal issues

The opening account of the importance of the accuracy principle for privacy protection should not lead the reader to believe that inaccurate personal data are not protected under general informational privacy provisions. On the contrary, the existing EU legal framework, for instance, does grant protection to 'inaccurate' data just as to any other personal data.[39] As explained, the individual to whom the data relate has the right to challenge it through the appropriate remedies,[40] and to have it rectified. What the individual does lack is, nevertheless, any right to have accurate personal data un-rectified.

The use of inaccurate data can be regarded as consistent with the right to privacy in different ways. It seems consistent with the right to respect for private life as protected by the European convention of human rights and fundamental freedoms (ECHR).[41] According to the case law of

[34] On the particular challenge that these practices represent for the EU legal framework, see: Hildebrandt and Gutwirth (2008).

[35] For a more detailed description, see: Dinant et al. (2008).

[36] Danna and Gandy (2002, p. 379).

[37] More information is available at: http://www.last.fm.

[38] See, for instance: Weitzner et al. (2006).

[39] 'Personal data' has been defined as "any information relating to an identified or identifiable natural person ('data subject'), in the understanding that "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" [see Article 2(a) of Directive 95/46/EC and reference in Article 2 of Directive 2002/58/EC].

[40] Article 29 Working Party (2007, p. 6).

[41] Council of Europe (1950). Note that the EU must generally respect the fundamental rights as guaranteed by the ECHR by virtue of Article 6(2) of the Treaty of the European Union.

the European Court of Human Rights, that right is to be interpreted in a broad sense and includes the right to self-determination and personal autonomy,[42] as well the representation of one-self, both in relation with bodily integrity and the protection of the private sphere. Individuals are recognised by this right, thus, the right to determine by themselves how they want to be presented in public.[43]

The free determination by the individual of the degree of accuracy of personal data disclosed in certain circumstances appears to be also consistent with the EU right to the protection of personal data, particularly if fully envisioned in the light of informational self-determination. Some consider that the right to the protection of personal data as singularly suited to protect the conditions needed for the construction of the self, in an interpretation inspired by the German view of the right to informational self-determination.[44] Its potentialities as a facilitator of freedom of self-representation have been pointed out,[45] and it has been maintained that data protection laws can be instrumental in providing a protection against external fixations of identity.[46] This perspective can be linked to a trend to interpret the notion of informational self-determination in very wide terms,[47] which tends to surround the right to the protection of personal data by a user-control discourse emphasising its potential to place in the hands of individuals choices determining how they are presented and represented.

Nevertheless, a tension can be currently perceived between such a theoretical user-control approach and the reality of legal developments limiting the 'control' on data to the provision of 'accurate' data. The recognition of a right to 'rectify', and the absence of any recognition of a right to freely determine if data are better kept 'inaccurate', could paradoxically lead to the support of a right to say 'the truth', but only the truth, which counters the very logic that allegedly frames the right to data protection. The right to the protection of personal data would grant individuals the right to determine which data related to them can be processed, but seemingly refusing them the right to decide how accurate should such data be. From this perspective, a more vigorous defence of the possibility of using inaccurate personal data, even if only under certain conditions, appears to be more consistent with the aims ultimately pursued by the protection of personal data.

Ethical perspectives

The deliberate provision of inaccurate data can raise many different ethical questions. To argue in favour of the dissemination of false data could be considered to be ethically problematic if understood as an invitation to systematically lie when disclosing personal data. The aim of this article is not to encourage such practices, but rather to consider the privacy-enhancing potentialities of certain uses of inaccuracy. As such, it focuses on a particular issue, namely the deployment of profiling and data mining practices for security purposes, and the potential of inaccuracy for ethical responses in this context.

The deployment of predictive data mining techniques in the particular field of security has been outstandingly contentious. The main problem lies in the implementation of massive processing of personal data (often originally collected for other, totally unrelated purposes) in the name of security, and particularly in the name of the fight against terrorism, with unclear benefits in relation to the official objectives of the measures. Whereas the effectiveness of such practices for the provision of security is generally unproved, or proved only in confidential circles, it is manifest that they do have a daily effect in the management of mobility, allowing for 'filtering', sorting out[48] and, in general, discriminating between persons.[49]

An example is the use for law enforcement purposes of passenger name record (PNR) data of individuals. This data, which consists of personal information in relation to travels in commercial flights, and is originally collected by airline companies for commercial purposes, is transmitted to law enforcement authorities and then mined in the name of security concerns. The massive processing of personal data of thousands of individuals is used to determine who, or, more exactly, which 'categories' of individuals are to be considered as deviant, or 'potentially suspect', and therefore to be placed under reinforced surveillance, or stopped and searched. In a sense, the whole travelling population is co-opted into constructing the definition of 'suspected minorities' and incriminating the other; the population is transformed into a corpus to be analysed to allow authorities to discriminate the 'normal' from the 'not normal' (and, therefore, 'potentially suspect').

[42] See, in this sense; *Pretty v. United Kingdom,* no. 2346/02, §§ 61 and 67, ECHR 2002 III.

[43] See, in this sense: *Peck v. United Kingdom*, no. 44647/98, ECHR 2003-I.

[44] In this sense, it should be noted that the development of the EU right to the protection of personal data took place while Germany was developing the right to informational self-determination (Informationelle Selbstbestimmungsrecht'). The concept was officially established by the German Constitutional Court in 1983 in its landmark Census case (65 BVerfGE 1, decision of 15.12.1983). See also: Poullet and Dinant, op. cit., p. 25.

[45] Van Den Hoven (2005, p. 47).

[46] Van Den Hoven and Vermaas (2007, p. 289).

[47] Isabel-Cecilia Del Castillo Vázquez (2007, p. 621).

[48] Lyon (2003).

[49] See, on these practices: De Goede (2008). See also: Ham and Atkinson (2002).

When the use of data mining for security purposes is discussed, it is relatively common to mention the principle of accuracy. Decision-makers regularly insist on the importance of the data processed being accurate,[50] and 'poor data quality' is often highlighted as the strongest obstacle to a widespread deployment of data transfers for law enforcement purposes.[51] Indirectly, the message transmitted is that we must all contribute to the general accuracy of data available in all fields, to increase effectiveness of security measures.

This argument is misleading. It implies, indeed, that there could be such a thing as a near perfect, permanent accuracy of personal data that would allow for data collected, for instance, for commercial purposes, to be later used for any other, unrelated purposes. It is a fact, however, that personal data are only meant to be accurate for the purposes for which they are to be processed. Thus, arguments about unsatisfactory accuracy serve only to mask the real problem with these measures: that data collected for one purpose should not be used for unrelated purposes. Predictive data mining strategies tend to systematically violate the principle of purpose limitation, which is another key standard of fair information practices, and which is, actually, the one that should be applied more carefully in order to ensure protection for individuals—not a deformed understanding of 'accuracy'.

Additionally, the argument also hides the fact that laws should provide for the necessary checks and balances to avoid any unjust decisions being taken based on the automatic processing of any set of data, regardless of how apparently accurate such data might be.[52]

Ethically, the issue emerges as to whether we as individuals agree with the use of predictive data mining for security practices or not. This ultimately touches upon the question of whether we agree with the screening of our daily lives for the purposes of defining who is to be categorised as deviant and 'potentially suspect', and thus placed under reinforced surveillance. If individuals are unambiguously given the possibility to originally determine which data they provide, and how accurate is it to be, they might be able to ethically decide how (and if) they want to contribute to allow for these practices to be deployed. By spreading inaccuracies irrelevant in the context of the application used but potentially relevant in other situations, individuals can reduce the use of the data provided for unexpected purposes. The provision of 'inaccurate' data can be interpreted as a preventive limitation against undesired secondary processing, a natural obstacle to further processing or a '*sticky policy*' promoting compliance with the purpose limitation principle. In this perspective, respecting the right to freely provide inaccurate data could be a tool to allow for ethical choices regarding the construction of the other.[53]

[50] See, for instance: European Commission (2005, p. II).

[51] Levi and Wall (2001, p. 194).

[52] See, in this sense: Cate (2008), Taipale (2007).

Concluding remarks

This article has identified a series of possible functions of inaccurate data as a privacy-enhancing tool. Without claiming that the use of such data is totally unproblematic, it suggests that recognising its potential could be more consistent with certain contemporary understandings of privacy and informational privacy. More concretely, it argues that there are reasons to be distrustful of any legal approaches that may reduce the potential of employing 'inaccurate' data in a privacy-enhancing manner. In this sense, as this article has sought to demonstrate, it is of special relevance to clarify that accuracy is an obligation for those processing data, but—except in certain circumstances—not an obligation for individuals. I has also tried to emphasise that through negotiations related to the disclosure of personal information can be served objectives which are not specifically individualistic or self-centred, but refer to how we want society to deal with the other, and how this is especially true in the age of predictive data mining.

Acknowledgments The author would like to express her sincere gratitude to Mireille Hildebrandt and Robin S. Dillon for their very kind encouragement and critical comments on some of the ideas expressed in the article. The author also thanks the two anonymous referees for their insightful comments and suggestions on earlier versions.

References

Article 29 Working Party. (2007). Opinion 4/2007 on the concept of personal data, WP136, 01248/07/EN. Brussels, adopted on 20 June 2007.

Bygrave, L. A. (2002a). *Data protection law: Approaching its rationale, logic and limits*. The Hague: Kluwer Law International.

Bygrave, L. A. (2002b). Privacy-enhancing technologies: Caught between a rock and a hard place. *Privacy Law & Policy Reporter, 9*, 135–137.

Cate, F. H. (2008). Government data mining: The need for a legal framework. *Harvard Civil Rights-Civil Liberties Law Review (CR-CL), 43*(2), 435–489.

[53] Interestingly, it is in the context of the classification into groups that the idea of 'self-identification' as a kind of free-determination of personal data has been more appraised. As racial and ethnic identity do not correspond to a 'biological truth', it is believed that it is up to the individuals to decide to which group they correspond, and the practice of collecting data on the basis of self-declared affiliation is generally encouraged, in line with the notion of individual self-determination. On this subject, see: Ringelheim (2006).

Charter of Fundamental Rights of the European Union. (2000). *Official Journal of the European Communities, C 364*, 1–22.

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 19 June 1990.

Council Act. (26 July, 1995). Drawing up the Convention based on Article K.3d of the Treaty on European Union on the establishment of a European Police Office. *(Europol Convention), Official Journal, C 316*.

Council Decision. (28 February, 2002) Setting up Eurojust with a view to reinforcing the fight against serious crime. *Official Journal, L 63*, 1–13.

Council of Europe. (1950). *European convention for the protection of human rights and fundamental freedoms as amended by protocol no. 11*. Rome, 4 Nov 1950.

Council of Europe. (1973). *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*.

Council of Europe. (1974). *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*.

Council of Europe. (1981). *Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series*, no. 108, 28 Jan 1981.

Council of Europe. (1981). *Explanatory report to the Convention for the protection of individuals with regard to automatic processing of personal data*. European treaty series, no. 108, 28 Jan 1981.

Danna, A., & Gandy, O. H, Jr. (2002). All that glitters is not gold: Digging beneath the surface of data mining. *Journal of Business Ethics, 40*, 373–386.

De Goede, M. (2008). The Politics of Preemption and the War on Terror in Europe. *European Journal of International Relations, 14*, 161–184.

De Hert, P., & Gutwirth, S. (2006). Privacy, Data Protection and Law enforcement, opacity of the individuals and transparency of power. In Erik Claes, Antony Duff, & Serge Gutwirth (Eds.), *Privacy and the criminal law* (pp. 61–104). Antwerp, Oxford: Intersentia.

Dinant, J. -M., Lazaro, C., Poullet, Y., Lefever, N., & Rouvroy, A. (2008). *Application of convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD). Expert report for the consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data.* Council of Europe: Strasbourg, 11 Jan 2008.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *Official Journal, L 201*, 37–47.

Directive 95/46/EC of the European Parliament and 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, L 281*, 31–50.

European Commission. (2005). *Impact assessment annex to the proposal for a council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters*. Commission Staff Working Document, COM(2005) 475 final, 4 Oct 2005.

European Commission. (2007). Communication from the commission to the European parliament and the council on promoting data protection by privacy enhancing technologies (*PETs*). COM(2007) 228 final, 2 May 2007.

Gallup Organization. (2008). *Data protection in the European Union: Citizens' perceptions*, Analytical Report, Flash Eurobarometer 225, Feb 2008.

Gutwirth, S. (2002). *Privacy and the information age*. Lanham: Rowman & Littlefield Publishers.

Ham, S., & Atkinson, R. D. (2002). *Using technology to detect and prevent terrorism*. Washington, DC: Progressive Policy Institute.

Hildebrandt, M., & Gutwirth, S. (Eds.). (2008). *Profiling the European citizen*. London: Springer.

Hustinx, P. (2005) Data protection in the European Union. *Privacy & Informatie, 2*, 62–65.

Isabel-Cecilia Del Castillo Vázquez. (2007). *Protección de datos: cuestiones constitucionales y administrativas (El derecho a saber y la obligación de callar)* (p. 621). Cizur Menor: Aranzadi, Thomson Civitas.

Kargupta, H., Datta, S., Wang, Q., Sivakumar, K. (2003). On the privacy preserving properties of random data perturbation techniques. In *Proceedings of the Third IEEE International Conference on Data Mining*, pp. 99–106.

Lenhart, A., & Madden, M., (2007). *Teens, privacy & online social networks: How teens manage their online identities and personal information in the age of MySpace* (p. ii). PEW Internet & American Life Project: Washington, DC, 18 April 2007.

Levi, M., & Wall, D. S. (2004). Technologies, security and privacy in the post-9/11 European Information Society. *Journal of Law and Society, 31*(2), 194–220.

Liu, L., Kantarcioglu, M., & Thuraisingham, B. (2008). The applicability of the perturbation based privacy preserving data mining for real-word data. *Data & Knowledge Engineering, 65*, 5–21.

Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk and digital discrimination*. New York: Routledge.

Lyon, D. (Ed.). (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.

Marx, GT. (2003) A tack in the shoe: Neutralizing and resisting the New Surveillance. *Journal of Social Issues, 49.* http://web.mit.edu/gtmarx/www/tack.html. Accessed at 2 Aug 2008.

Online Computer Library Center, Inc. (OCLC). (2007). *Sharing, privacy and trust in our networked world: A report to the OCLC membership*. Dublin: Ohio, 29 Oct 2007.

Organization for Economic Co-operation and Development (OECD). (1980). Guidelines on the protection of privacy and transborder flows of personal data, adopted in the form of a recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data. Paris, 23 Sep 1980.

Pfitzmann, A, Hansen, M. (2008) Anonymity, unlinkability, undetectability, unobservability, pseudonimity, and identity management—a consolidated proposal for terminology. Version v0.31, 15 Feb 2008.

Poullet, Y., & Dinant, J. -M. (2004). Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications: L'autodétermination informationnelle à l'ère de l'Internet. Report for the Comité Consultatif de la Convention pour la Protection des Personnes à l'Egard du Traitement Automatisé des Données à Caractère Personnel. Council of Europe, Strasbourg, 18 Nov 2004.

Ringelheim, J. (2006). *Processing data on racial or ethnic origin for antidiscrimination policies: how to reconcile the promotion of equality with the right to privacy?* Center for Human Rights and Global Justice Working Paper, No. 13. New York, 2006.

Taipale, K. (2007). *The privacy implications of government data mining programs*. Testimony before the US Senate Committee on the Judiciary.

Van Den Hoven, J., (ed.). (2005). *Managing identity, privacy & profiles*. Alter Ego Deliverable 1.3. SOTA Delft Technical University, Delft, 25 May 2005.

Van Den Hoven, J., & Vermaas, P. E. (2007). Nano-technology and privacy: On continuous surveillance outside the panopticon.

Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine, 32(3), 283–297.

Weitzner, D. J., Abelson, H., Berners-Lee, C. H., Hendler, J., Kagal, L., McGuinness, D. L. et al. (2006) *Transparent accountable data mining: new strategies for privacy protection*? Computer Science and Artificial Intelligence Laboratory Technical Report, Massachusetts Institute of Technology.

William, B., & Chiasson, M. (2005). If Fair Information Principles are the answer, what was the question? An Actor-Network Theory Investigation of the Modern Constitution of Privacy. *Information and Organization, 15*(4), 267–293.

Yuste., O. E. (2001). The relevance of the data protection principles set out in the Convention and its Additional Protocol. In Council of Europe. In *Proceedings of the European Conference on Data Protection on Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data: present and future,* Warsaw, Nov 2001, p. 56.