PERSONAL DATA PROTECTION MODELS: ASPECTS OF OWNERSHIP

George Bouchagiar¹ and Maria Bottis²
¹ Attorney-at-law, Tutor-Research Fellow on Data Protection/JP, Ionian University, Kaloheratu 14, Corfu, Greece, 49100
² Associate Professor on Information Law, Ionian University, Ioannou Theotoki 72, Corfu, Greece, 49100

ABSTRACT

The potential application of a property rights model to personal data is an old subject of legal discussion. As some scholars have argued, such treatment could strengthen individuals' control over their information or could put pressure on firms to better manage people's data. Given that in the modern era personal data does have some economic value and is treated as a digital asset, this article mentions some examples to detect uncertainties that have, under current norms, occurred. Furthermore, it studies the status of personal data after a person's death and points out some common features that the concept of such data possession and the concept of ownership share. Finally, several shortcomings of the proprietary-based model are discussed to draw particular attention to the sensitive character of our information and its relation with the fundamental principles of human value and dignity.

KEYWORDS

Personal Data, Ownership, Deceased, Property Right

1. INTRODUCTION

Let us assume that George and Stella are friends. They live in different countries and meet once a year. They are about to meet on the 28th of January 2019. George sends an e-mail announcing the date of his arrival and Stella "scrutinizes" their previous e-mails to find places, where they have been before, and pick the best one to go for a drink with George. While scrutinizing their digital conversations, Stella finds a five-years-old e-mail concerning an old bickering. Five years ago, George behaved in an inappropriate manner, but Stella forgave him. But now that she remembers George's previous behavior, she changes her mind. Old digital conversations do not let her forgive George, nor do they let her forget her friend's previous behavior (Mayer-Schönberger 2009).

In present-day societies, digital remembering is the default. However, we need to remember to forget. We may need to think beyond laws and not turn into an unforgiving society. The fact that digital data did not let Stella forget and forgive might not be that dangerous. However, in other occasions, things could be worse.

In 2013, Jetpac collected the content of 150 million images uploaded on Instagram in order to create a digital collection list of businesses¹. Photographs, taken in e.g. a restaurant, which contained faces with lipstick, were classified by Jetpac's algorithm and, thus, the place was characterized as "dressy". In cases where people in the photograph were only men, the algorithm characterized the places as "gay bars". Many Instagram images had also geo-location information and, hence, by having collected, analyzed and processed all above data, Jetpac could have created a list of all e.g. gay bars of Tehran.

Publishing such a collection would be a service or a disservice?

It would certainly be welcomed by a homosexual citizen or visitor of Tehran, who would not risk asking anyone, and perhaps the wrong person, to find the above gay bars. However, consequences would probably be devastating for Tehran's homosexual community, if this collection fell into the hands of the mullahs.

Some authors argue that a property rights model could apply to personal data (under the General Data Protection Regulation (GDPR)), persona data is any information relating to an identified or identifiable natural person) to strengthen control of the data subject over her private information (Lessig 2006; Liebenau 2016). This model could also enable individuals to share profits from data’s exploitation and force firms to make better decisions on the collection and use of such data (Samuelson 2000). Could this model apply to personal data, under current laws and norms?

2. CURRENT EU – US DATA PROTECTION REGIME

Under the European regime, the right to the protection of personal data is protected as a fundamental human right (Article 8(1-2) of the Charter of Fundamental Rights of the European Union, Article 16(1) of the TFEU). It is an established position of jurisprudence that the Convention for the Protection of Human Rights and Fundamental Freedoms does not protect a right to obtain remuneration for the waiver or sacrifice of a fundamental human right; European courts hold that human rights reflect personal integrity and liberty and, hence, one could conclude that there is no space for a property approach (E.C.H.R., Mellacher v. Austria, 1989, 12 E.H.R.R. 391; Nadezhdina 2009). This means that, in accordance with the above positions, privacy, as a human right inseparable from personhood, cannot be waived or transferred (Prins 2006 at pp. 234-237). However, there have been cases, in which the European Court of Human Rights held that an individual may consent to waiving a fundamental right, albeit to do so in an explicit manner (Deweer/Belgium, ECHR, 27 February 1980, A35 par. 48-54; De Wilde, Ooms, Versyp/Belgium, ECHR, 18 June 1971, A12 par. 65; Lawson 1997).

Contrary to the European regime, the American legislator has adopted a “piecemeal” (Bottis 2012) approach that can be found in several Acts, such as the Fair Credit Reporting Act (1970, 15 U.S.C. § 1681), the Electronic Communications Privacy Act (1986, 18 U.S.C. § 2510), the Cable Communications Policy Act (1984, 47 U.S.C. § 551) or the Video Privacy Act (1988, 18 U.S.C. § 2710). In the United States, privacy (Warren, Brandeis 1890; Cavoukian, Tapscott 1997) is protected under a torts model (Restatement (Second) of Torts §§ 652A-652E, 1972). As some authors have argued, a common law tort could be used not only to enforce accountability on data traders but also to provide remedies for individuals, who have suffered harm to their privacy interests of choice and control (Ludington 2006). Other academics argue that people should own their personal information and be entitled to control what is done with it and that the tort solution might be preferable to a property rights approach, which however would likely offer only modest protection (Litman 2000).

Setting aside EU and US approaches, some economists and scholars argue that personal data could emerge as a new asset class in itself (World Economic Forum 2011; Manovich 2011) and speak of data’s economic value, which is indeed measurable (Malgieri, Custers 2017; OECD 2013; Chirita 2016; European Data Protection Supervisor 2014). Such approaches are in accordance not only with some old academic opinions, that view commercialization of personal data as a potential way to strengthen individuals’ control over data (Samuelson 2000), but also with some international institutions’ views, which have recently recognized that personal data may be provided or used as money in exchange for the supply of digital content and digital services.

Given that in present-day society “tout s’achète” (Beigbeder 2000; Förster, Weish 2017), in this paper we study the status of personal data after a natural person’s death and we highlight some common features that “traditional” ownership (Becker, 1980) and “personal data possession” share. We also discuss several shortcomings of the proprietary-based model to draw particular attention to the sensitive character of personal data and its relation with the fundamental principles of human value and dignity.

---


3. PERSONAL DATA AFTER DEATH

As we shift from atoms to bits (Mayer-Schönberger, Cukier 2014), digital assets, with economic or personal value, have emerged. For example, a domain name certainly has some financial value, while an e-mail may have emotional value. But let us focus on personal data and examine its status, as a digital asset, after an individual’s death.

The European Data Protection Directive¹ does not mention anything about the data of the deceased and, hence, some European Member States decided to protect it. For instance, under Bulgarian law, in case a natural person dies, her rights of access may be exercised by heirs, who are enabled, amongst others, to request, at any time and free of charge, from the personal data controller a confirmation as to whether or not data relating to the deceased are being processed, information as to the purposes of such processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed (Article 28(3) of Bulgarian Law For Protection Of Personal Data).

Moreover, under Estonian law (Chapter 2 of the Estonian Personal Data Protection Act), the consent of a data subject shall remain valid during the lifetime of the data subject and for thirty years after the death of the data subject, unless the individual has decided otherwise. Interestingly, in Estonia, after the death of a natural person, processing of personal data relating to the deceased is permitted only with the written consent of the successor, spouse, descendant or ascendant, brother or sister of the data subject.

On the other hand, the General Data Protection Regulation focuses on living persons and does not apply to personal data of the deceased (Member States, however, may provide for rules regarding the processing of personal data of deceased persons, recital 27 of GDPR). By ignoring the deceased, one could argue that the GDPR leaves no space for a proprietary model. However, it should be noted that the GDPR’s title refers not only to the protection of natural persons with regard to the processing of personal data, but also to the free movement of such data.

Could essential features of ownership be detected in the European concept of personal data possession?

4. DATA AS PROPERTY: IN WHOSE HANDS?

An essential element of the notion of ownership is the right to possess. This means that a person has the right to exclusive control of the thing (Becker, 1980). In case of intangible items, possession may be understood metaphorically. With regard to personal data, one of the fundamental principles of data protection law is respect for personal autonomy (Bottis 2014). Legal provisions, concerning such data, safeguard rights to informational self-determination (Kang et al. 2012). Thus, it has been consistently supported by authors that the right to the protection of personal data refers to control by the subject over the processing of her data (Oostveen, Irion 2016; Rengel 2014).

Another feature of ownership is the right to use, meaning the right to personal enjoyment of the benefits of the thing, other than those of management and income (Becker 1980). One could claim that a user has the right to use and to enjoy the benefits deriving from her personal data, e.g. e-mail or her IP address or “cookies” (Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Jun. 20, 2007; Opinion 1/2008 on data protection issues related to search engines, April 4, 2008). Besides, by using “cookies”, companies offer “the best experience” and, thus, consumers enjoy the “benefits of the thing”.

Furthermore, the right to manage, to decide how and by whom a thing should be used (Becker 1980), can also be detected in the concept of possession of personal data. Namely, the key tool for a legal control of personal data is the subject’s consent (Solove 2013; Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, July 13, 2011) to its processing. Consent of the data subject is defined as any freely given, specific, informed and unambiguous indication of the individual’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Article 4(11) of GDPR). Thus, it would be fair to argue that the data subject has the right to manage her information and decide how and by whom her information should be used.

Another important element of ownership is the right to the income—that is to the benefits deriving from personal use of an item and allowing others to use it (Becker 1980). At this point, things get complex. It is companies, rather than data subjects, that process data, and, thus, have the “right to the income” from this processing. However, some authors argue that consumers should have the right to know the value of their data (Malgieri, Custers 2017). Hence, if such rights were established, users might then be able to participate in profits. In any case, after having provided her data, a consumer does enjoy some kind of benefits, such as the innumerable “free” digital services.

Moreover, while obligations to delete personal data are also provided under Data Protection Directive (e.g. Articles 6(1)(e) and 12(b) of DPD), the GDPR establishes the right to erasure (‘right to be forgotten’, Flaherty 1998; Blanchette 2002; Dodge, Kitchin 2007; Mayer-Schönberger 2009), which is defined as the right of an individual to obtain from the controller the erasure of personal data, concerning him or her without undue delay (Article 17(1) of GDPR). This right resembles the right of the owner to destroy a thing (Becker 1980; Koops 2011).

Another crucial feature of ownership is the right to modify the thing, to effect changes less extensive than annihilation. Indeed, an individual has the right to modify her e-mail address or her name.

In addition, the right to alienate or to abandon ownership reminds us of cases De Weer/ Belgium (ECHR, 27 February 1980) and De Wilde, Ooms, Versyp/Belgium (ECHR, 18 June 1971), where the European Court of Human Rights held that an individual may consent to waiving a fundamental right.

The need for free flow of personal data illustrates some kind of utilitarian approach and data portability has been strongly supported by the European legislator. Thus, an individual has the right, amongst others, to transmit her personal data to another controller without hindrance from the controller to which these data have been provided (Article 20(1) of GDPR). This resembles the right to transmit, to devise or bequeath the thing (Honoré 1961).

One of the main principles relating to processing of personal data is that the latter shall be processed in a manner that ensures appropriate security of the personal data, including the protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5(1)(f) of GDPR). This seems to resemble two features of ownership, i.e. the right to security—that is to immunity from expropriation— and the prohibition of harmful use -one’s duty to forebear from using the item in ways harmful to oneself or others (Becker 1980).

Ownership lasts, in theory, forever (Becker 1980); but the protection of data, not. However, if we examine personal data in a sui generis right database, then we could argue that protection of personal data may indeed last for an eternity (Davisson 2006; Bottis 2004; Boyle 2003), in favor, however, not of the data subject but, of the database maker.

Another feature of ownership is liability to execution, to having the thing taken away as payment for a debt (Becker 1980). Here, again, it is firms, rather than individuals, which may have data taken away as payment for a debt: in fact, in recent years, some companies had no other choice than to sell their clients' personal data as a way of silencing creditors (Enos 2001; Prins 2006, at p. 228), while in other occasions, databases that contained personal data changed hands and ownership during strategic company movements (Gautheronet 2001).

Finally, residuary rules govern the reversion to another, if any, of ownership rights, which have expired or been abandoned (Becker 1980). Such rules are, for example, those that determine the disposition of property left by intestate deaths. Such rules could resemble the provisions of the above Bulgarian and Estonian personal data protection laws.

To sum up, one could argue that the notion of ownership and the concept of personal data possession do share common features. However, with regard to certain of these features, personal data, as quasi property, has perhaps fallen into the wrong hands.
5. DISCUSSION

The right to the protection of personal data was a “wonderful idea” of an era, when information was rarely shared, societies were local and communications were expensive. In current era, when a pandemonium of information is circulated online, digital societies have no frontiers and communications are inexpensive, we may need to rethink models for protecting such fundamental human rights. A proprietary model might not resolve all the problems, albeit the treatment of the right to personal data as a quasi property right could remind people that an individual is the owner of—and the one entitled to control—her data and that she has the right and the human need to forget.

As a possible disadvantage of our approach here, one could note that a personal and a property model derive from dissimilar sources and concepts, which perhaps should not blend. A quasi property right in our case should not signal that a human being is equal to an object, since anything that is personal to us should normally not be subject to ownership. If such particular distinction is not as clear as it can be in law, then human dignity, the constitutional and fundamental principle upon which the right to the protection of personal data is indeed based, could be threatened. Moreover, the unambiguous identifier of our dignity, our self-determination, should always play a key role in these potential approaches of privacy, given that it is the feature that enables the individual to freely make decisions about her life.

The main GDPR’s objective, as we see in its title, is to strike a fair balance between the protection of individuals with regard to the processing of their personal data and the free movement of such data (e.g. recital (10) of GDPR). We do observe, on the other hand, the European legislator’s wish to treat individuals’ information as a highly protected moral good, incapable of being subject to ownership or any kind of measurement. This illustrates the direction, towards which the EU regime is heading, which is, of course, different than a pure ownership approach that would regard data as a mere object. However, we stress the GDPR’s provisions on data portability and free flow of data in general. These provisions strongly support, to us, a quasi property right, if the appropriate attention is also drawn to human dignity and self-determination in the interpretation of all GDPR provisions.

REFERENCES


228


