Property rights in personal data

Purtova, N.N.

Published in:
Computer Law and Security Review

Publication date:
2009

Document Version
Early version, also known as pre-print

Property rights in personal data: Learning from the American discourse

Nadezhda Purtova

Tilburg Institute for Law, Technology, and Society, The Netherlands

ABSTRACT

This contribution is an attempt to facilitate a meaningful European discussion on propertization of personal data by explaining the idea as it emerged in its 'mother-jurisdiction', the United States. The piece starts with an overview of how the current US legal system addresses the data protection problem and whether, according to the US commentators, the law does it effectively. Furthermore, the contribution presents propertization of personal information as an alternative to the existing data protection regime and one of the ways to fill in the alleged gaps in the US data protection system. The article maps the US propertization debate. Pro-propertization arguments are considered from economic perspective as well as from the perspective of the limitations of the US legal and political system. In continuation it analyses proposals on how property rights in personal data would have to be regulated, if at all, in case the idea of propertization is accepted. The main points of criticism of propertization are also sketched. The article concludes with a brief summary of the US propertization discourse and, most importantly, with a list of the lessons Europeans can learn from their American counterparts engaging in the debate in the home jurisdiction. Among the mane messages is that the outcome of the debate depends on the definition of the problem propertization is called on to tackle, and that it is the substance of the actual rights with regard to personal data that matters, and not whether we label them as property rights or not.

Keywords: US information privacy law, data protection, scope of property rights, property in personal data

1. Introduction

US scholars have been debating whether personal information should be viewed as property since the early 70s.[1] Propertization would acknowledge the existing phenomenon of commodification of, or a high market value attributed to, personal data, and could offer a solution to the data protection problem - a result of the 20th century rise of private and government databases. The key dimensions of the data protection problem were recognized to be privacy as secrecy,[2] a bureaucratic way of handling information,[3] and the lack of control over personal information.[4] Introducing property rights in personal data arguably would address at least the aspect of the lost control. The natural rights theory has been also invoked to support property claims for personal information that implies a certain inherent connection

---

1 AF Westin, *Privacy and Freedom*, (1967)

2 Senate Floor debates, reprinted in U.S. Senate and House Committees on Government Operations, Legislative History of the Privacy Act of 1974, s. 3418 (PL 93-579), 94th Cong., 2d sess. (Washington, D.C.: Government Printing Office, 1976), p. 775

3 P Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, (1995) p. 72; DJ Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. R. 1393, p. 1421-22

4 E.g., AF Westin, *Privacy and Freedom*, (1967) p. 7; Solove 2001, p. 1428

between an individual and data pertaining to him.[5] Other commentators see benefits of propertization in a rhetorical value of property talks.[6] However, the most discussed approaches to information privacy as property have come from a utilitarian perspective[7] and from the perspective of the shortcomings specific to the US data protection system.

Notably, although the American debate on propertization of personal data has long exhausted itself,[8] only a few European commentators ever reflected on the idea of propertization.[9] Today, however, there is an apparent need to develop a European perspective on the propertization of personal data. Firstly, the commodification of personal information – one of the staring points of the propertization debate - occurred in Europe, too. Secondly, the problem of the lost control over personal information has received renewed attention on the EU level. An example of such attention is a 14 April 2009 video message of Vivian Reding, the EU Commissioner for information Society and Media, where she said that "Europeans must have the right to control how their personal information is used, and […] that the Commission would take action wherever EU Member States failed to ensure that new technologies such as behavioural advertising, RFID 'smart chips' or online social networking respected this right."[10] Ownership of data is one of the tools at the disposal of law to give individuals the desired control. Therefore, the subject of propertization of personal information is worth revisiting.

This contribution is an attempt to facilitate a meaningful European discussion on propertization of personal data by explaining the idea as it emerged in its 'mother-jurisdiction', the United States. In other words, this paper does not intend to offer a ready-to-use European perspective on the possibility of property rights in personal data. Neither does this piece argue for or against introduction of property rights in personal data. Instead, the reader should consider the contribution as a step just preceding a full-blooded European discussion,[11] an attempt to look back at the past debate overseas and rehearse lessons learnt there to have initial points of reference when starting the European debate. In particular, it seems to be of great importance to make the reader aware of the many faces of property that appear in the US propertization argument, each 'face' defended from a different perspective, bearing a different meaning and performing a different function. With this purpose in mind, this paper will try to go beyond an obvious insight normally present in a comparative study, *i.e.* that when trying on the US-born idea of propertization of personal information Europe cannot be blindly guided by the US debate but needs to develop its own view. Instead, the paper will show that, in the US discourse, propertization of personal information was expected to perform certain functions, namely, to overcome shortcomings of the current US

---

5 Solove 2001, p. 1446 (although he does not develop the natural law argument further); V Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information" (2003) U.C. Davis L. Rev. 37 379, p. 430; MJ Radin, "Property and Personhood" (1982) 34 Stanford Law Review 5 957, p. 959

6 "Property talk is just how we talk about matters of great importance" (L Lessig, "Privacy as Property" (2002) 69 Social Research: An International Quarterly of Social Sciences 1 247); "If you could get people (in America, at this point in history) to see certain resource as property, then you are 90 percent to your protective goal." (L Lessig, "Privacy as Property" (2002) 69 Social Research: An International Quarterly of Social Sciences 1 247)

7 Although this is a simplification, when applied to the argument for propertization, this article uses "utilitarian," "economic," and "instrumental" interchangeably.

8 Indeed, a reader will have difficulties finding relevant literature after 2004.

9 see, e.g. JEJ Prins, "Property and Privacy: European Perspectives and the Commodification of our Identity" in *The Future of the Public Domain, Identifying the Commons in Information Law*, (2006) 223-257

10 "Citizens' privacy must become priority in digital age, says EU Commissioner Reding" available online at <http://ec.europa.eu/information_society/newsroom/cf/itemlon>

11 A fool-blooded discussion on property rights in personal data from a European perspective is a subject of the author's further research.

data protection system (outlined in parts 2 and 3.2); to give individuals some control over personal information (parts 3.1.1 and 3.1.2), and generate incentives for companies in private sector to respect privacy, create privacy enhancing technologies and, as a result, a better system of data protection (part 3.1.3). Part 3.3 presents an outline of the ideas as to the scope of proposed property rights. It shows how different the propertization initiatives are with regard to the approaches to regulation and content of the proposed rights, and therefore suggests that what will matter in a future European discourse is the actual content of granted rights, rather than the 'property' label. Part 3.4 concludes the analysis of the US propertization debate with main points of criticism towards the idea of propertization, emphasizing again the importance in a discourse of the content of rights in personal data rather than a word used to call them, and raising a question of the necessity of an empirical study to (dis)prove some statements made in the US debate to support propertization. Part 4 ends the analysis by making an inventory of lessons the Europeans could learn before considering the possibility of property rights in personal data. Before the analysis starts, a disclaimer should be made that since the paper focuses on the US debate, it will draw primarily on the US authors.

2. The US information privacy law

The author of this contribution believes that the origin of the idea of propertization of personal information in the US largely lies in the inability of the American data protection law to adequately respond to (already not so new) challenges of the Information revolution. The function of property rights would have been to compensate for this handicap. The following section will explain why.

The US law on personal data protection requires an unfamiliar reader considerable effort to understand it. Its complexity stems from several sources. The first is terminology ambiguity. In Europe it is not common for textbooks and scholarly writings to refer to this body of law as the law of information privacy, or simply privacy law.[12] Second, although this choice of wording is not surprising given that the data protection problem in the US has been conceptualized as the one of privacy, it still reflects (or arguably leads to) some confusion when traditional mechanisms of privacy protection are applied to new personal data related problems.[13] Paul Schwartz and Joel Reidenberg brand this pattern as an attempt to put "new wine in old bottles."[14] Another source of complexity, especially in the eyes of a European reader, is that the US information privacy law does not have a single hierarchical order of rules but comprises norms of tort, constitutional, and statutory law - a patchwork of the rules different in sources, subjects of regulation, and applicability. Finally, the body of law at hand operates in the federalized legal system with competences divided between the federation and the states.[15] With no uniform hierarchical personal data protection law in place, Solove describes the US system of data protection as the one which "uses whatever is at hand [...] to deal with the emerging problems created by the information revolution."[16]

---

12 DJ Solove, Rotenberg, Marc; Schwartz, Paul M. , *Information privacy law*, (2006) p. 9; J Kang, Buchner, Benedikt, "Privacy in Atlantis" (2004) 18 Harvard Journal of Law and Technology 1 229, p. 231, etc.

13 Solove 2001;

14 PM Schwartz, Reidenberg, Joel R., *Data Privacy Law: A Study of United States Data Protection*, (1996) p. 102

15 Schwartz & Reidenberg, pp. 7-8

16 Solove 2001, p. 1430

The subsequent sections introduce the US information privacy law system;[17] explain how it operates, which areas of the data protection problem it addresses, and what gaps the commentators see in the patchwork of the US information privacy law which have to be filled in, arguably by propertization.

2.1 Tort law

It has been widely acknowledged that tort law has played a groundbreaking role in the protection of privacy in the US.[18] In their 1890 renowned article[19] Warren and Brandeis derived a right to privacy from the common law torts. However, the role of torts in resolving the data protection problem is limited, both due to limited scope of individual torts and more systematic shortcomings common to torts as a common law institute. This section explains the point in more detail.

White defines the US torts as a field reflected in individual actions and concerned with civil wrongs not arising from contracts.[20] The tort law is mainly common law, *i.e.* it has been developed by courts, through the system of precedent.[21] That is, when ruling on a case, the courts rely on the previously decided similar cases. Yet, the binding force of precedent is limited in the US where the courts are "more willing [...] to develop the law in accordance with social reality."[22] Due to the constitutional division of federal and state powers, the US tort law is mainly state law.

Branching of the tort law among the states has resulted in "the numerous variations within different jurisdictions"[23] and "the lack of agreement on fundamental principles of the common-law system"[24] causing overall difficulties in administering justice. To overcome those, The American Law Institute[25] produced the Restatement of the Law of Torts, regarded as "a very significant attempt at a searching and exhaustive analysis of the entire field."[26] The Restatement is not binding. Its role is comparable to that of scholarly writings in the international law.[27] Yet, it is "the most complete and thorough consideration which tort law ever has received,"[28] and, in considering the US privacy torts, this study will rely on the Restatement.

The Restatement distinguishes four kinds of privacy torts: (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private

---

17 The overview of law is not complete and goes as far as it is sufficient to prove the point of this part of the paper: to introduce the propertization argument as it goes in the US in light of the legal background against which the argument emerged.

18 DJ Solove, Rotenberg, Marc; Schwartz, Paul M. , *Information privacy law*, (2006) p. 9

19 Warren and Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)

20 GE White, *Tort law in America : an intellectual history*, Expanded ed (2003) p. xxiii

21 R Michaels, "American Law (United States)" in JM Smith (ed) *Elgar Encyclopedia of Comparative Law*, (2006) 66-78 p. 68-69.

22 K Llewellyn, *The Common Law Tradition*, (1960)

23 Official web-site of the American Law Institute available online at <http://www.ali.org/index.cfm?fuseaction=about.creationinstitute> (accessed on November, 18th, 2008)

24 Ibid.

25 Ibid.

26 WPP Keeton, William Lloyd, *Prosser and Keeton on the law of torts*, 5th student ed. (1984) p. 17

27 P Blok, *Recht op Privacy*, (2002)

28 Prosser and Keeton on Torts, p. 17

facts; (3) publicity which places one in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[29]

The tort of intrusion protects against intentional intrusion, physical or otherwise, "into the solitude or seclusion, or private affairs or concerns," of another "in a manner that is highly offensive to a reasonable person."[30] The tort of intrusion has potential to provide a remedy against the data protection problem in part related to "an unauthorized acquisition or transfer of personal information."[31] Indeed, this tort has relevance for the intangible world of personal information since it does not require intrusion into one's home or other physically defined space, but can be of one's "personality" or "physical integrity."[32] However, in practice it is difficult to extend the intrusion tort to cover new information practices. The difficulties stem either from some conceptual characteristics of the tort, or from mere unwillingness of the courts to expand its boundaries.

There are several obstacles for the new information practices to constitute intrusion. First, intrusion must involve an invasion of "seclusion." Although the tort of intrusion does not require any physically defined private place, the courts have rejected claims when plaintiffs have been in public places.[33] As a result, a great share of the data protection problem remains not covered by the intrusion tort: information collection and use often occur in cyberspace many parts of which "may well be considered public places."[34]

Second, the intrusion should be unauthorized. The courts have interpreted this requirement as protecting only secret information. In *Dwyer v. Am. Express Co,*[35] a group of American Express cardholders challenged the profiling practices of the American express companies and their renting of the information regarding card-holders' spending habits. The American Express analysts composed the card-holders' profiles based on how they shopped, how much they spent, and on their behavioural characteristics and spending histories.[36] Plaintiffs argued that such practices involved disclosure of private financial information and resembled cases involving intrusion into private financial dealings, such as bank account transactions.[37] The court refused to classify the information practices involved as intrusion, because the plaintiffs did not establish that the intrusion was unauthorised: "[b]y using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analysed, will reveal a cardholder's spending habits and shopping preferences."[38] In other words, mere compiling and renting information voluntarily disclosed by the plaintiff to the respondent, or creation of new information on the basis of the voluntarily revealed data (profiling) does not constitute intrusion.[39]

The third obstacle is the division between different kinds of information based on the level of secrecy. The courts, e.g. in *Remsburg,*[40] distinguished between information that may be reasonably expected to remain private even after disclosure to a third party and information

---

29 Prosser, *Privacy* 48 Cal. L. Rev. 1960 p.389

30 American Law Institute, §652B (1977)

31 Bergelson, p. 405; see also Solove 2001, p. 1432

32 *Phillips v. Smalley Maint. Servs*., 435 So. 2d 705, 711 (Ala. 1983) cited in Bergelson. p. 406. The case-law analysis in the section on Torts is mainly drawn from the works of Daniel Solove and Vera Bergelson.

33 *Muratore v. M/S Scotia Prince*, 656 F. Supp. 471, 482-83 (D.Me. 1987) cited in Solove 2001, p. 1432

34 Solove 2001, p. 1432

35 *Dwyer v. Am. Express Co.*, 652 N.E. 2d 1351, 1352-53 (Ill. App. Ct. 1995)

36 *Dwyer*, at 1353

37 Ibid, at 1354

38 Ibid.

39 Ibid.

40 *Remsburg v. Docusearch, Inc.*, 816 A. 2d 1001 (N.H. 2003)

that is not so "secret".[41] The court had to decide whether obtaining a person's social security number from a credit reporting agency without plaintiff's knowledge or consent, and obtaining her work address[42] constituted intrusion. The *Remsburg* court classified social security number as the information that may be reasonably expected to remain private even after its disclosure to the third party and work address – as not so "secret, secluded or private." Only in the first case may a plaintiff maintain a cause of action for intrusion.[43] According to Daniel Solove's analysis of the case-law, the courts have rejected the intrusion claims involving the types of information that are most likely to be subject of collection into the databases:[44] unlisted phone numbers,[45] selling subscription lists to direct mail companies,[46] collecting and disclosing an individual's past insurance history,[47] etc.

Fourth, the use of the tort of intrusion in the context of the data protection problem is limited by the requirement that the information practice has to be highly offensive to a reasonable person.[48] In determining whether the intrusion was sufficiently offensive, one has to take into account "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[49] Daniel Solove points out that the "highly offensive to a reasonable person" requirement is difficult to satisfy in the individual case,[50] especially, because "each particular instance of collection is often small and innocuous;"[51] and the required level of danger is created only "by the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time."[52]

Finally, even provided the above-mentioned shortcomings are corrected, due to the nature of intrusion, the applicability of this tort to the data protection problem would be limited only to data collection.[53]

The tort of disclosure of private facts is committed when publicity is given "to a matter concerning private life of another [...] if the matter publicized [...] would be highly offensive to a reasonable person, and is not of legitimate concern to the public."[54] Similar to the tort of intrusion, this tort "could conceivably be applied to certain uses of databases, such as the sale of personal information by the database industry."[55] However, it is highly unlikely that these practices would meet the requirements established by the prevalent case-law.

Publicity is the first such requirement. For a transfer of data to constitute a disclosure, the information must be communicated "to a sufficient number of people, so that it is

---

41 *Remsburg* at 1004-05

42 Ibid.

43 *Remsburg*

44 Solove 2001, p. 1432

45 *Seaphus v. Lilly*, 691 F. Supp. 127, 132 (N.D. Ill. 1988)

46 *Shibley v. Time, Inc*., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975)

47 *Tureen v. Equifax, Inc*., 571 F.2d 411, 416 (8th Cir. 1978)

48 see, e.g., *Remsburg*

49 *Remsburg*, at 1008-09

50 Solove 2001, p. 1432

51 Ibid.

52 Ibid.

53 Bergelson, p. 406; WJ Fenrich, "Common Law Protection of Individuals' Rights In Personal Information" (1996) 65 Fordham L. Rev. 951, at 972 n.150; JR Reidenberg, "Privacy in the Information economy: A Fortress or Frontier for Individual Rights?" (1992) 44 Fed. Comm. L. J. 195, at 222-223

54 Restatement §652D

55 Solove 2001, p. 1433

"substantially certain to become [...] public knowledge."[56] However, the sale of personal information normally is limited to a transfer from a primary to a secondary collector.

Further, both standard of "highly offensive" and "highly personal" information, often interrelated in actual cases, are difficult to satisfy. The disclosure tort protects only "highly personal information", *i.e.* it "is not intended for the protection of any shrinking soul who is abnormally sensitive about such publicity."[57] Disclosure becomes highly offensive when it concerns personal facts that are not open to public eye, and kept by plaintiff "entirely to himself or at most revealed only to his family or to close friends."[58] In part concerning information open to a public eye, one may extend Solove's concern with regard to the tort of intrusion. Even if a plaintiff can prove a highly personal and embarrassing character of the disclosed information, there will be no cause of action if she happened to reveal this information in cyberspace often regarded as public.

Similarly, the disclosure tort does not protect against publicity of the facts in the public record "such as the date of birth, the fact of his marriage, his military record, the fact that he is admitted to the practice of medicine or is licensed to drive a taxicab."[59] However this information is routinely used for profiling. As Vera Bergelson concludes, the disclosure of merely neutral facts would not be actionable.[60] In most cases the lifestyle information, along with names[61] and places of work and residence,[62] is not regarded as "highly personal and embarrassing."[63]

The third obstacle is that the level of protection afforded by the tort of disclosure is linked to the social conventions - "the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbours and fellow citizens."[64] However, the problem is that those habits and socially adopted standards of 'normal' in data processing have been altered by the very technological and marketing developments which the social norms are invoked to restrain.

Finally, it is difficult for a plaintiff to make use of even afforded protection. According to Solove, it is hard "to discover that such sales or disclosures have been made."[65] By design, Solove continues, the tort of private facts serves to redress excesses of the press, and consequently deals with the widespread dissemination of personal information in ways that naturally become known to the plaintiff, whereas "the use and sale of databases is often small and done in secret."[66]

The tort of false light protects against "publicity to a matter [...] that places the other before the public in a false light" that is "highly offensive to a reasonable person."[67] The commentators agree that this tort has limited or no applicability to the data protection problem. Apart from the publicity and "highly offensive" requirements addressed earlier, there are several obstacles specific to the false light.

---

56 Restatement §652D, comment a.

57 W Prosser, "Privacy" (1960) 48 Cal. L. Rev. 383, p. 397; *Forsher v. Bugliosi*, 608 P.2d 716, 723 (Cal. 1980)

58 Restatement §652D, comment b.

59 Ibid.

60 Bergelson, p. 409

61 *King County v. Sheehan*, 57 P.3d 307, 316 (Wash. Ct. App. 2002)

62 *Webb v. City of Shreveport*, 371 So. 2d 316, 319 (La. Ct. App. 1979)

63 Bergelson, p. 410

64 Restatement §652D, comment c.

65 Solove 2001, p. 1433

66 Ibid.

67 Restatement §652E

First, false light protects one's reputation,[68] whereas data processing is rarely harmful to this interest.[69] Second, Bergelson sees no applicability of the false light to the data processing where the individuals provided relevant information themselves. The defining element of this tort is that the revealed information is false or erroneous, whereas personal information transferred by primary to the secondary collectors usually has been provided by the data subjects themselves and is correct. Bergelson speculates that a set of information, or a profile that is the subject of the transfer, may be limited or one-sided and thereby put an individual in false light.[70] Yet, she concludes, this argument leads to the absurd possibility of banning all information transfers because "no information is 'complete'."[71] Only when information was not provided by the individual, the courts apply this tort to protect against dissemination of erroneous information "when the defendant has not taken proper steps to ensure its correctness."[72]

A certain information practice is actionable under the appropriation tort if it consists of exploitation of "the name or likeness of another" to defendant's "own use or benefit."[73] Literature distinguishes between appropriation and the right of publicity. According to Prosser, the difference between the appropriation tort and the right of publicity results not from the actions that gave rise to a complaint but rather from "the nature of the plaintiff's rights and the nature of the resulting injury. [...] [W]hile he appropriation branch of the right of privacy is invaded by an injury to the psyche, the right of publicity is infringed by an injury to the pocketbook." [74] Virtually every state recognizes either one of the two wrongs, often making no difference between the two.[75] This study also considers them together.

Commentators agree that this tort has potential to provide a remedy against the use of personal information for targeted marketing if regarded as the use of one's name to profit.[76] Three recent cases - *Shibley v. Time Inc*.,[77] *Dwyer*, and *U.S. News and World Report v. Avrahami*[78] - are usually considered as attempts to bring the appropriation suit against the practices of unauthorized dissemination of personal information through the sale of mailing lists. However, the courts seemed unwilling to extend the applicability of the appropriation to new information practices, and those attempts have failed. *Shibley* was a class action brought in Ohio against a number of journals and the issuer of American Express credit card who sold the lists of subscribers without their prior consent to direct mail companies. The court saw no action for appropriation because the plaintiff was not used to endorse any product.[79] In *Dwyer* (Illinois) the court found that in case of subscription lists "an individual name has value only when it is associated with one of defendants' lists"[80] and that "defendants create value by categorizing and aggregating these names."[81] In *Avrahami* the Virginia court maintained that "the tort of appropriation is intended only to give redress to a person whose name, portrait, or picture was used for either advertising or trade."[82] In *Remsburg* the New Hampshire Supreme Court refined the requirement by stating that the appropriation necessitates the benefit from

---

68 Prosser, p. 400
69 Solove 2001, p. 1433
70 Bergelson, p. 405, fn 143
71 Ibid.
72 Ibid.
73 Restatement §652C
74 Prosser, Law of Torts §117, p. 401, fn 154:
75 Bergelson, p. 410;
76 Solove 2001, p. 1433-34; Bergelson, p. 411
77 *Shibley v. Time Inc.*, 341 N.E.2d 337, 340 (Ohio Ct. App. 1975)
78 *U.S. News and World Report v. Avrahami,* No.95-1318, 1996 Va. Cir. LEXIS 518 at *1 (va. Cir. Ct. June 13. 1996)
79 *Shibley*, at 339
80 *Dwyer,* at 1356
81 *Dwyer,* at 1356
82 *Avrahami* cited in Bergelson, p. 412

the "reputation, prestige or other value" associated with the person,[83] and "does not protect one's name per se."[84] An appropriation claim was rejected against a private investigator that provided his client with personal information of a woman subsequently stalked and killed by that client since the benefit did not result from the victim's reputation, but from the client's willingness to pay.[85] Because the key element of the cause of action in appropriation is reputation, prestige or other value associated with a name, the appropriation tort is most effective at protecting celebrities who have created value in their personalities,[86] but not average individuals.

Leaving aside proposals to fix the shortcomings of privacy torts by creating a new cause of action against ill information practices, inherent limitations to the common law of tort still do not allow creation of a general system of data protection solely on their basis. Among those limitations are inhomogeneous and unsystematic character of torts,[87] protection of only negative rights,[88] etc. With regard to the latter, the task of creating positive rights or imposing affirmative obligations – as some claim, essence of data protection[89] - is alien to the nature of tort law itself. Tort law is concerned with providing a remedy against already committed civil wrongs and as such can not create positive rights and does not have a preventive function.[90]

2.2 Constitutional law

Some authors assign to the United States Constitution[91] a special role of "the starting point to understanding of the right to privacy"[92] in the US. Historically, the first 'privacy right' was the right against unlawful searches and seizures protected by the Fourth Amendment[93] Yet, the Constitution plays a limited role in the information privacy system. To understand why, one has to obtain insight into the place of this document in the US legal order.

Apart from establishing the federal government, the idea behind adoption of the US Constitution was to protect the American people from possible tyranny by limiting government powers.[94,95] That influenced the scope of all constitutional rights, including constitutional protection of information privacy. First, the constitutionally protected privacy interests limit only government actions. Data processing by private entities is not subject to

---

83 *Remsburg*, at 1009

84 *Remsburg*, at 1009 (see also Restatement §652C, comment d.)

85 *Remsburg*, at 1010

86 Solove 2001, p. 1434

87 Michaels, p. 71

88 Bergelson, p. 415

89 De Hert, P., Gutwirth, Serge (2003). "Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies. Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview," European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE).

90 Bergelson, p. 415

91 The major points of the discussion are applicable to the state constitutions of the states. E.g. although a number them expressly protect privacy rights (e.g. Arizona Constitution, art.II, para.8; California Constitution, art.I, para.1; Illinois Constitution, art.I, para.6), they limit only government activities. (Reidenberg 1992: p. 208, fn 61; Schwartz & Reidenberg p.9)

92 JQ Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) Yale L.J. 113 1151, p. 1211-12

93 Ibid.; K Gormley, "One Hundred Years of Privacy" (1992) Wis. L. Rev. 1335, pp. 1358-59

94 Schwartz & Reidenberg, pp. 6, 29

95 This doctrine is generally referred to as "state action" and is explained in a series of the US Supreme Court decisions, e.g. *DeShaney v. Winnebago County Department of Social Services*, 487 U.S. 189 (1989)

the constitutional constraints.[96] Second, although the Constitution prevents certain government actions, it imposes no positive duties, e.g. to create data protection system, or minimum information privacy protection.[97] Finally, the emphasis on limiting government rather than citizens creates, as Schwartz and Reidenberg put it, "a basic regulatory philosophy that favours the free flow of information,"[98] that, as one may think, is rather in line with the image of the US as a liberal state.

The U.S. Constitution knows no express right of privacy, let alone information privacy. The sources of the protection in the field are constitutional amendments interpreted by the U.S. Supreme Court.[99] The provisions most referred to are the Fourteenth Amendment's Substantive Due Process Clause, the Fourth and the Fifth Amendment.[100]

First section of the Fourteenth Amendment, referred to as Substantive Due Process clause, prohibits deprivation of any person's "life, liberty, or property, without due process of law."[101] It raises the question whether deprivation "is justified by a sufficient purpose [...] [or] whether there is a sufficient substantive justification"[102] for it. Courts have been using Substantive Due Process to safeguard rights that are not enumerated in the constitution,[103] including information privacy.

The U.S. Supreme Court found privacy, first in the contraception and abortion cases, covered by the concept of personal liberty as secured by the Fourteenth Amendment.[104] In 1977 *Whalen v. Roe* decision[105] the Supreme Court extended protection to personal data, recognizing "the individual interest in avoiding disclosure of personal matters."[106]

However, the significance of the Substantive Due Process for solving the data protection problem is diminished. First, as interpreted in *Whalen*, it protects only information privacy understood as non-disclosure of personal information. Second, ambiguous definition of the right at hand allows narrow reading of the clause, limiting protection to few kinds of personal information pertaining to an abstract notion of liberty.[107]

---

96 Solove 2001, p. 1435; Schwartz & Reidenberg, p. 6;

97 Solove 2001, p. 1435

98 Schwartz & Reidenberg, p. 6;

99 Ibid., p. 29

100 Ibid.; Solove 2001, p. 1435; GR Stone, Seidman, Louis M., Sunstein, Cass R. , *Constitutional Law*, 5th (2005) pp. 845

101 U.S. Constitution, I Am., s.1

102 E Chemerinsky, "Substantive Due Process" (1999) Toronto Law Review 15 1501, p. 1508

103 Chemerinsky, pp. 1505, 1509-10

104 *Griswold v. Connecticut*, 381 U.S. 479 (1965) (protection of decisional privacy with regard to contraception); *Roe v. Wade* 410 U.S. 113 (1973), at 153: the constitutional right to privacy is "broad enough to encompass a woman's decision whether or not to terminate her pregnancy."

105 429 U.S. 589 (1977); Justice Brennan, concurring, explained: "[Broad] dissemination by state officials of such information [...] would clearly implicate constitutionally protected privacy rights, and would presumably justified only by compelling state interests." Ibid, at 606

106 *Whalen*

107 *Kallstrom* 136 F.3d at 1059 (the Sixth Circuit found that undercover police officers have a constitutionally protected privacy interest in some personal information contained in their personnel files under the substantive due process clause); The information pertaining to "private sexual matters" was also found to "warrant constitutional protection against public dissemination." *Bloch v. Ribar*, 156 F.3d 673, 686 (6th Cir.1998); yet, the correctional officers' social security numbers were not found sufficiently sensitive information to be under constitutional protection despite threat of retaliation (Barber v. Overton, 496 F.3d 449, 456 (6th Cir.2007)).

Under the Fifth Amendment, "[n]o person [...] shall be compelled in any criminal case to be a witness against himself[...]."[108] Thereby the Amendment establishes a privilege against self-incrimination, and prohibits the government from compelling individuals to disclose incriminating information about themselves. This way the Fifth Amendment limits the government's power to collect information.[109]

However, apart from the obvious limitation of applicability only in criminal proceedings, the provision at hand does not create general protection of information privacy or a guarantee of non-disclosure. It only protects against the "compelled self-incrimination."[110] That is, the Fifth Amendment does not prevent the government from requiring a person to produce papers and records.[111] Nor does the Amendment protect against subpoenas for personal records held by third parties (e.g. private sector data collectors). In short, the Amendment is about protection of a person in a criminal case, not personal data *per se*.[112]

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[113] The Amendment limits the government power to collect information as a search or seizure.[114] Yet, the provision at hand does not fully address the data protection problem.

The pattern of the IV Amendment privacy jurisprudence from *Boyd v. United States,*[115] (1886) to *Olmstead v. United States*[116] and *Katz v. United States*[117] resulted in a widely used test of a reasonable expectation of privacy. Under the test, the Amendment affords protection if (a) a person exhibits an "actual (subjective) expectation of privacy" and (b) the expectation is one "that society is prepared to recognize as 'reasonable.'"[118]

The main criticism of the Amendment's protection is that it relies on the understanding of privacy as secrecy,[119] "a discrete commodity, possessed absolutely or not at all."[120] The second point of criticism pertains to the "reasonable expectation of privacy" standard. Solove et al point out that the standard is not objectively verifiable since the courts do not rely on empirical evidence of what the society is prepared to recognize as reasonable.[121] Besides, the threshold of what society is prepared to consider reasonable or normal is changing, and after the 9/11 events has been "under renewed scrutiny"[122]

To sum up, the attempts to address personal data protection problem by constitutional means fail both for the reasons of the limited function of the US Constitution, and arguably erroneous conceptualization of the problem. However, commentators also agree that it cannot be expected from the Constitution to offer a detailed solution to the data protection problem.

---

108 U.S. Constitution, V Amendment

109 Solove et al, p. 208

110 *Fisher v. United States*, 425 U.S. 391 (1976)

111 *Shapiro v. United States*, 335 U.S. 1 (1948)

112 C*ouch v. United States*, 409 U.S. 322 (1973)

113 US Constitution, IV Amendment

114 Solove et al, p. 208

115 *Boyd v. United States*, 116 U.S. 616 (1886) hereinafter referred to as *Boyd*

116 277 U.S. 438 (1928)

117 389 U.S. 347 (1967)

118 389 U.S. 347 (1967)

119 Solove 2001, p. 1435

120 L Tribe, *American Constitutional law* 2nd (1988) at 1391 quoting Justice Marshall's dissent in *Smith v. Maryland*, 442 U.S. 735 (1979)

121 Solove et al, p. 251

122 FH Cate, Litan, Robert "Constitutional Issues in Information Privacy" (2002) 35 Mich. Telecomm. Tech. L. Rev. 9 35,

It only sets a framework for solution and leaves the rest for political process.[123] The following section focuses on the products of that process – information privacy legislation.

2.3 Statutory protection

Federal government responded to the increased public concerns pertaining to the new information practices first in 1973 when the HEW Committee issued a report *Records, Computers, and the Rights of Citizens*.[124] The report contained a proposal of a Code of Fair Information Practices establishing five basic principles: ban on secret personal-data record-keeping systems; an individual must be able to find out what information pertaining to him has been collected and how it is used; an individual must be able to prevent the information pertaining to him from being used for the purpose other than the one for which it has been collected; an individual must be able to correct or amend a record of identifiable information about him; and finally, a data-processing organization must assure the reliability of and take reasonable precautions to prevent misuse of the data.[125]

The Code acknowledged the separate essence of the idea of *information* privacy.[126] The assumption behind the Fair Information Practices was that not preventing information collection but "delineating fairness in information practices would protect individual privacy."[127]

The US commentators agree on a significant role the Code played in formulating the information privacy standards.[128] However, it is not directly binding and its significance was diminished in the course of implementation. Under the pressure from public and private organizations, legislative initiatives ended with the passage of weakened legislation.[129] Public sector organizations (government agencies) argued that that extensive regulation would inhibit effectiveness of their operation. Private sector entities testified that the compliance with the regulations would be disproportionally burdensome given that there was little evidence of information abuses in private sector.[130] What the US data processing legislation represents now is a system with inherent gaps: with no independent supervisory authority,[131] where public and private sector data processing have been treated separately. The 1974 Privacy Act regulating public sector processing is a reduced version of the initially proposed omnibus law (s. 3418), although generally in line with the Fair Information Practices,[132] whereas private sector data processing is almost entirely left for self-regulation, with the exception of a number of statutes, like the Video Privacy Protection Act of 1988 and the Right to Financial Privacy Act of 1978, adopted as a reaction to particularly shocking incidents of data mishandling.[133] The commentators concur that the regulation of the private sector data processing in the US is reactive rather than anticipatory, ad hoc rather than

---

123 Schwartz & Reidenberg, p. 29

124 Regan 1995, p. 75-76

125 U.S. Dep't of health, Educ. & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems* 29-30, 41-42 (1973) ("HEW Report")

126 Regan 1995, p. 75-76; emphasis added

127 Ibid., p. 76-77

128 Regan 1995, p. 76-77

129 Ibid., p. 78

130 Ibid., p. 78; U.S. Senate Committee, *Privacy*, pp. 515, 450-451

131 Although several civil liberties offices have been created since September, 11, 2001, the US privacy experts agree that "these [...] are not structurally independent of the government bodies that they are responsible for overseeing; and they do not have the power to investigate and sanction privacy violations." (pp. 1, 7)

132 Bignami 2007 discusses the weaknesses of the Act.

133 Regan 1995, pp. 5-7

systematic and comprehensive.[134] To be fair, one should mention more recent area-specific legislation in the field of data protection, e.g. regarding children's data, financial data and health data (HIPPA). However, although these have definitely been received as improvements, they address only certain sectors of data processing and the problem of the absence of omnibus law establishing uniform data protection standards for private sector remains unsolved.

Correcting regulatory shortcomings in a systematic way and creating such an omnibus law is considered unlikely given a strong lobby of information industries in the US Congress, and a conflict between data protection and free speech interest which is routinely resolved in favour of the latter.[135]

3. Correcting shortcomings of the US data protection system via propertization

As follows from part two of this paper, the current US data protection law offers virtually no tools to return control of personal data to individuals. This is especially so in case of the private sector data processing. The criticism of the US information privacy law has been followed by numerous proposals aiming to fix the shortcomings of the system. The most established ones are retooling the system of torts,[136] more regulation, and, finally, propertization of personal information. The latter has gained even more attractiveness in the eyes of its proponents given the already mentioned flaws of the first two: peculiar nature of torts and lobbying power of the information industries in the US context. This section shows how property rights in personal data are argued to be able to perform where other solutions, arguably, fail, *i.e.* to give the control over personal data back and create a better system of data protection in general.

To get a more structured insight into the US argument for propertization, it makes sense to divide the subject of property in personal data into three distinct issues. First, whether personal information should be regarded as an object of property rights. The second issue naturally follows from a positive answer to the first question and is with whom - individuals (data subjects), or data collectors - property rights should be vested. The third issue is, after property rights are introduced, what the default rules (if any) are that should govern their transfer.[137]

Ironically, with regard to the first issue both information privacy opponents and privacy advocates argue for and against propertization, albeit for different reasons. Representatives of the information industry argue for propertization as a means to legitimize and facilitate already existing market of data. On the other hand, Judge Richard Posner, an opponent to privacy and advocate of uninterrupted flow of information, argues against. For Posner property rights in personal information provide a means of withholding true information from the marketplace and are therefore inefficient.[138] Some privacy advocates concur with Posner in his conclusion but for a different reason, i.e. that personal data is different from other

---

134 See e.g. Regan 1995, pp. 5-7,CJ Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? " in PEAM Rottenberg (ed) *Technology and Privacy: The New Landscape* (1997) Solove 2001, p. 1440, etc.

135 e.g. *U.S. West v. Federal Communications Commission*

136 The proposal has been briefly considered in the section concerning privacy torts.

137 However, consistent with the aim of this article to consider the American idea of propertization as a way of personal data protection, this contribution focuses on the argument for creating individual property rights in personal information and default contractual rules.

138 The only instance when property rights in personal data are justified is when it will foster more efficient transactions (RA Posner, *the Economics of Justice*, (1981) at 235). It may be argued though that Posner is not against property rights in true personal information *per se*, but against vesting them with the individuals – data subjects.

objects and cannot be treated as property.[139] There are data protection proponents who regard property regime as optimal for ensuring information privacy. Although, a remark should be made here that the privacy advocates do not tend to spend much time arguing in favour of propertization *per se*, but, like Murphy, presume that personal information "like all information, is property"[140] and immediately move to the discussion on who should own it.[141]

When the need for property rights in personal data is agreed upon, the standpoints of the information privacy advocates and opponents are much clearer in defending who should be the owner of the data. Advocates of data protection stand for the allocation of this resource to the data subjects, whereas proponents of disclosure argue for vesting property with data collectors. According to Julie Cohen, "opponents of strengthened privacy protection think of collection of personally-identified data as 'their' property; as evidence, they point to their investment in compiling the databases and developing algorithms to 'mine' them for various purposes."[142] Those opponents of the unchained information market are consistent to argue against the need for any default contractual rules governing the data transfers since the market already functions optimally.[143] To show how property, arguably, is able to give control of personal information back to data subjects, the following analysis will focus only on the arguments of privacy advocates.

Although, as it has been already mentioned, the idea of propertization may be defended from the perspective of natural rights and rhetoric effects, most commentators in favour of property in personal data base their arguments on the economic analysis and specific shortcomings of the current US system of data protection.

3.1 Economic argument for propertization

Roughly, the US commentators engaging in the economic analysis of law see property as a tool facilitating market exchange which, provided transaction costs are minimal, will achieve optimal privacy by balancing the value of personal information to a company against the value of the information to the individual and the larger social value of data protection.[144] This perspective receives three interpretations by the US information privacy scholars. Each of them will be considered in more detail shortly. As a result, it will be shown that, despite the fact that the validity of the instrumentalist perspective is not limited to the United States, all three interpretations of the instrumental argument are difficult to divorce from the US context,

---

139 See e.g. P Samuelson, "Privacy as Intellectual Property?" (2000) 52 Stan. L. R. 1125, , Schwartz & Reidenberg, DJ Solove, "Conceptualizing Privacy" (2002) 90 Cal. L. Rev. 1087, , J Litman, "Information Privacy / Information Property" (2000) 52 Stan. L. R. 1283,

140 RS Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy" (1996) 83 Geo. L.J. 2381, pp. 2383-84

141 Ibid.,

142 Cohen 2000, p. 1378 referring to Harris S. Gordon, Steven J. Roth, Scott J. Lieberman, Ann Zeller & Anne McConnell, *Customer Relationship management: A Senior management Guide to technology for Creating a Customer-centric Business* <http://www.the-dma.org/library/publications/customerrelationship.shtml>)

143 Privacy in Commercial World, 106th Cong. (2001) (statement of Paul H. Rubin, Professor of Law and Economics, Emory University School of Law), available at <http://www.house.gov/commerce/hearings/0301200143/Rubin66.htm.> (accessed on November 18th, 2008); Direct Marketing Ass'n, Inc., Consumer Privacy Comments Concerning the Direct Marketing Association Before the Federal Trade Commission (July 16, 1997); Fred H. Cate, Privacy in the Information Age 113 (1997)

144 Solove brings as examples of such an approach John Hagel III & Marc Singer, *Net Worth: Sharing Markets When Consumers Make the Rules* 19-20 (1999) (advocating for an "infomediary" between consumers and vendors who would broker information to companies in exchange for money and goods to the consumer); Paul Farhi, *Me Inc: Getting the Goods on Consumers*, Wash. Post, Feb. 14 1999, at H1]

namely, US-specific understanding of property, specific weaknesses of the US information privacy, and the specifics of the US legal system in general.

The three interpretations of the utilitarian argument for propertization are (1) argument for individual property rights in personal data as opposed to default disclosure rule, (2) property as opposed to torts, and, finally, (3) property as a means to create incentives to apply privacy enhancing technologies (PETs).

3.1.1 Individual property as opposed to disclosure

Some of US scholars argue in favour of the individual property in personal data based on the dichotomy between privacy rule (*i.e.* control) and a disclosure (absence of privacy) rule. Mostly, their argument stems from the assumption they make that personal information *is* property, and assigning it to an individual, within their framework of analysis, is the only alternative to the absence of information privacy whatsoever. The argument by Richard S. Murphy illustrates this line of thought. Murphy merely presumes that personal information, as any information, is property. The question Murphy focuses on is then "who owns the property rights to such information--the individual [...], the person who obtains the information, or some combination?"[145] Depending on to whom the property right is assigned initially: an individual or a data collector, Murphy distinguishes two kinds of default rules: non-disclosure (or privacy rule) and disclosure. The substance of the privacy (non-disclosure rule) is that "the individual can control dissemination of (or has a partial property right in) information deemed "private," but not in other information.[146] Under a disclosure rule, control over personal data is initially assigned to a data collector.[147] Within Murphy's analytical framework, to have an individual property right in personal information is the only alternative to no information privacy at all.

Murphy does not hold a preference to any one of those two rules since for the achievement of maximum utility, initial assignment of the resource - personal data - does not matter. A party, who values the resource most will always negotiate in his or her favour, provided the transaction costs are minimal.[148] However, since the latter is not the case in a real world, the law in the form of default contract rules or tort should intervene and allocate the initial entitlement. Murphy engages in an instrumental analysis of privacy and concludes that "there are, also, substantial economic benefits to personal privacy."[149] Since in the utility calculus, not only financial but also some psychic values like shame, or a mere taste for privacy count, non-disclosure may be more efficient than a default disclosure,[150] "Limiting disclosure of information may be whenever the individual concerned values his privacy highly, for any reason other than to deceive."[151] That implies that Murphy's defence of non-disclosure holds only for some sorts of personal information and in particular circumstances, when disclosure will negatively influence the quality and quantity of information (and they are both vital for the efficient transactions). The examples of such special circumstances the relationships between a doctor and a patient, a client and an attorney, a state and a rape victim, etc.[152] A newspaper should be found liable for the violation of a property right of a rape victim when it

---

145 Murphy, pp. 2383-84

146 Ibid.

147 Ibid, pp. 2388

148 Here Murphy relies on the Coase Theorem as explained in RH Coase, "The Problem of Social Cost" (1960) J.Law & Econ. 3 1, in RS Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy" (1996) 83 Geo. L.J. 2381, fn 85

149 RS Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy" (1996) 83 Geo. L.J. 2381, p. 2416

150 Ibid., p. 2416

151 Ibid., p. 2387

152 Ibid., pp. 2409-10

reports her true name. The rationale is that the state has an interest in prosecuting rapists. If the state does not maintain confidentiality of the victims, they will not report crimes,[153] similar to the patients who will not disclose to physicians information vital for their treatment, or defendants who will be discouraged to fully cooperate with their attorneys.

Jerry Kang also argues that vesting property right in personal information with individuals (*i.e.* giving the control back) as opposed to the firms would be a more efficient solution. First, if the initial entitlement is given to a data collector, the data subjects would incur substantial costs to find out what information has been collected and used. The collector, to the contrary, would not face extra costs since it already possesses the knowledge on what information was collected and how it was treated. Second, unlike the collector, the individuals would face a collective action problem. The companies would not respect individual privacy preferences because it would be prohibitively expensive to tailor new information practices for every data subject. Therefore, individuals would have to unite their effort. In the process "they would suffer the collective action costs of locating each other, coming to some mutual agreement and strategy, proposing an offer to the information collector and negotiating with it – all the while discouraging free riders."[154]

This is a basic utilitarian argument in favour of privacy guided by the considerations of efficiency, and would as such be valid in the settings other than the US. What makes it hard to divorce from the American context is the understanding of property it rests upon. Neither of the two authors gives definition of property in favour of which he argues. Murphy only says that one way of securing control over personal information is when "[i]ndividual can control dissemination of (or, put another way, has a partial property right in) certain information."[155] This definition of the scope of property rights as applied to personal data corresponds to the popular definition of the data protection problem as the one of the lack of control. But besides that, it seems to be rooted in the notion of property as explained in the 1972 article by Guido Calabresi and A. Douglas Melamed[156] and now considered standard by the US commentators.[157] Calabresi and Melamed define property by contrasting it to the liability rules. "An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller,"[158] whereas "whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule."[159] Some commentators read this definition of property as implying "an exclusivity axiom," i.e. that an owner has a legitimate claim to exclude the rest of the world from his property.[160] That is, property is ensuring that the entitlement (in the case at hand – information privacy) is protected, whereas the liability's function is seen as to make sure that transfer of the entitlement is possible even without a holder of the entitlement, against an objectively determined compensation. As Lessig puts it, "property protects choice; liability protects transfer."[161]

---

153 Ibid., pp. 2410

154 J Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stan. L. R. 1193,

155 Murphy, p. 2384

156 G Calabresi, Melamed, A. D., "Property rules, liability rules, and inalienability: one view of the cathedral" (1972) Harv. L. Rev. 85,

157 See, for instance, RA Epstein, "A Clear View of the Cathedral: the Dominance of Property Rules" (1997) 106 Yale L.J. 2091, p. 2091

158 G Calabresi, Melamed, A. D., "Property rules, liability rules, and inalienability: one view of the cathedral" (1972) Harv. L. Rev. 85, Calabresi & Melamed, p. 1092

159 Ibid.

160 PM Schwartz, "Property, Privacy, and Personal Data" (2004) 117 Harv. L. Rev. 7 2055,

161 L Lessig, *Code and other laws of cyberspace*, (1999)

Understanding the US argument for propertization from the angle of Calabresi and Melamed's definition of property makes it clear that within this analytical framework only property regime offers some degree of control and protection to personal data. Any alternative (liability) rule only secures transfer of personal data, *albeit* against some objectively defined compensation. The remaining versions of the utilitarian argument for propertization rest on the same understanding of property.

3.1.2 Property as opposed to torts

The second interpretation of the utilitarian argument for propertization is offered by e.g. Vera Bergelson.[162] She argues in favour of propertization on different grounds, among others, that property regime would cure the weaknesses of the current system of privacy torts. Bergelson argues that "the choice between the tort regime and the property regime for the protection of personal information means the choice between property rules and liability rules as defined [...] by Calabresi and Melamed."[163] Indeed, when a system of privacy torts is in place, they allow collection of personal information just like a liability rule allows transition of a resource. Tort remedy is available only *post factum* and has no preventive function. The value of transmitted personal data is determined not by the holder of the entitlement, i.e. an individual, but by the court. Bergelson brings a utilitarian argument similar to Murphy and Kang's that propertization "affords the individual maximum control over personal information and allows all interested parties to enter into mutually acceptable transactions without tying up the valuable societal resources."[164] Her distinct contribution to the utilitarian debate, however, is in two points. First, the preference for torts (i.e. the liability rule) as opposed to property implies that "individual entitlements to personal information [...] would have to be enforced by litigation, on a case-by-case basis, which would involve considerable expenditures of funds and time."[165] Second, since the compensation under the liability rule is defined by the state, "the plaintiff will have to prove actual damages, which most likely will be trivial. That by itself will discourage people from bringing lawsuits against those who violate their rights in personal information, thereby making the rule inefficient."[166]

3.1.3 Property as an instrument to create a general system of personal data protection

There is another group of the US authors defending propertization from an instrumentalist standpoint, though of a different nature. Their main concern is not efficiency, but creation of the overall system of data protection comprising law, technology and market tools which interaction can ensure proper level of information privacy. Namely, Julie Cohen speaks of law as only a mechanism to create incentives to build a general privacy infrastructure: "Law can and should establish a new set of institutional parameters that supply incentives for the design of privacy-enhancing technologies to flourish. Legal protection alone cannot create or guarantee information privacy."[167]

Lessig is probably the most outspoken commentator within this group. He also brings an economic argument that property rules would permit each individual to decide what information to disclose and protect "both those who value their privacy more [...] and those who value it less."[168] However, Lessig only uses economic analysis as a building block of his

---

162 V Bergelson, "It's Personal, but Is It Mine? Toward Property Rights in Personal Information" (2003) U.C. Davis L. Rev. 37 379,

163 Ibid., p. 417

164 Ibid., p. 419

165 Ibid., p. 417

166 Ibid., pp. 417-18

167 J Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan. L. R. 1373, pp. 1437-38

168 L Lessig, *Code and other laws of cyberspace*, (1999)

own theory of privacy protection in the information age, as explained in the book *Code and Other Laws of Cyberspace*[169] and its revise version *Code 2.0.* First, he argues pretty traditionally, information privacy is in essence control over personal information. Second, unlike in the real world, the architecture (or "code") of a cyberspace makes collection of information and control over that information, difficult for lay people. Third, such an architecture is a result of human activity and, therefore, can be altered.[170] Fourth, the US information processing practices are based on self-regulation, *i.e.*, there is no general legislation requiring businesses to alter this architecture and use privacy-friendly technologies. Nor is there motivation to account for interests of the individuals. In absence of property interests, the companies make use of personal data for free. However, if individuals had property rights in personal data, it would force businesses to negotiate with the individuals, account for their interests, and alter the architecture, i.e. invest into development of PETs. The individual privacy would be better secured, not only by law but by interaction of the latter, market mechanisms and technologies.[171]

Cohen shares Lessig's views that interaction of law, market, and technology can create conditions for individuals to exercise meaningful control over personal information.[172] She believes that information privacy protection may learn from copyright where technology already offers means to secure property rights that were difficult to protect in the past.[173] Cohen refers to Phil Agre who described 'technologies of identity' which made it possible to prevent collection of personal data.[174]

> *The same technologies that enable distributed rights-management, she continues, functionally might enable the creation of privacy protection that travels with data – obviating the need for continual negotiation of terms, but at the same time redistributing "costs" away from individuals who are data subjects.*[175]

One cannot deny the potential benefits technology offers to information privacy protection. However, Lessig's argument must be treated with care. Apart from general criticism of the propertization argument explained further in the paper, the weakness of his theory is that one of Lessig's basic assumptions (the reliance of the current data protection system on self-regulation and absence of general regulation of personal data processing) is purely American.[176]

3.2 Propertization argument pertaining to the specificities of the US legal system

Along with various interpretations of the utilitarian argument for propertization, some commentators favour the property rights in personal data as they could overcome the limitations of the US information privacy system.

---

169 Ibid.,

170 point also made by Cohen in J Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan. L. R. 1373, p. 1437

171 L Lessig, *Code and other laws of cyberspace*, (1999)

172 J Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan. L. R. 1373, 1391

173 Ibid, p. 1391

174 PE Agre, Rotenberg, Marc eds., *Technology and Privacy : the New Landscape*, (1997)

175 Cohen 2000, p. 1391

176 Besides, some other US scholars, in particular, Mark Rotenberg, disagree with the idea that the US data protection rests on self-regulation and criticize Lessig's theory on that basis (M Rotenberg, "Fair Information Practices and the Architecture of privacy (What Larry Doesn't Get)" (2001) 1 Stan. Tech. L. Rev.,)

Murphy argues that protecting information privacy as a property right will revive the current system of the US privacy torts. For Murphy, one of the reasons why the tort system fails to protect personal data is that when a court comes to balance First Amendment free speech interests of the press against some vaguely defined privacy interest, free speech naturally wins. That would not happen to privacy defined as constitutionally protected property.[177]

Besides, propertization of personal data will respond to the individual preferences for privacy in a more sensitive way than the current tort system does. Privacy torts operate with some objective standards of privacy whereas this is not an objective but a subjective standard which has to be protected. In privacy cases, Murphy argues, "strictly speaking, 'norms of civility' are irrelevant [for calculating utility]" since "the depth and diversity of privacy preferences are highly variable across individuals" and "the objective approach will often get the balance of preferences wrong." [178]

Another factor in favour of propertization is that the change in law would not have to go through the federal legislative system which, either due to the constitutional limitations or influence of the lobby showed itself unproductive when it comes to regulating privacy. Jessica Litman who otherwise is opposed to the idea of propertization, admits that the appeal of this solution relies on the fact that "property rights can be recognized as a matter of state common law without invoking the federal regulatory machinery, which seems too helpless, pernicious, or corrupt (depending on your political persuasions) to offer a meaningful solution."[179]

3.3 Scope of property rights: default rules

Another key issue in the US propertization discourse is the scope of property rights in personal data, limited or unlimited by default rules. When describing the range of views on this matter in the US discourse, this section will show that despite a label of property attached to possible sets of rights in personal data, what really matters is not the name, but the content of the rights. Indeed, the proponents of the market solutions insist on the widest scope of the rights possible, whereas privacy advocates supporting propertization argue for certain default rules. The main discussion is focused on alienability, or a possibility to sell personal data, which is somebody's property, freely. Full alienability and absolute inalienability being two opposites on a continuum, other options lie in between ranging from more intensive to ad hoc regulation.

As the information industry's representatives are against individual ownership of personal data, they reject any idea of regulating transactions, including the default rules. According to the "market purists," as Solove names them,[180] the market already accounts for privacy concerns.[181] To the extent that consumers want their privacy protected, the market responds to this demand and accounts for it in its utility calculus. Indeed, the industries have been adopting privacy policies in response to the consumers' privacy concerns. If privacy is not

---

177 Murphy, p. 2388

178 Ibid, p. 2388

179 J Litman, "Information Privacy / Information Property" (2000) 52 Stan. L. R. 1283,

180 DJ Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. R. 1393,

181 In describing the purists' argument Solove refers to Privacy in Commercial World, 106th Cong. (2001) (statement of Paul H. Rubin), available at <http://energycommerce.house.gov/reparchives/107/hearings/03012001Hearing43/print.htm> (accessed on November 18th 2008); Direct Marketing Ass'n, Inc., Consumer Privacy Comments Concerning the Direct Marketing Association Before the Federal Trade Commission (July 16, 1997); Fred H. Cate, Privacy in the Information Age 113 (1997)

sufficiently protected in other cases, it means that people value efficient and convenient transactions, custom-tuned service, etc. more.[182]

When it is agreed that property rights in personal information should be vested with the data subject, the information privacy proponents continue to develop default contractual rules that would govern market transactions enabled by propertization. However, as Solove points out, propertization proponents are "certainly not in agreement over the types of property entitlements and contractual default rules that should be required."[183] The literature is divided already on the issue whether the rules should be of a contractual nature, i.e. whether the parties may negotiate for a different set of rules. Pamela Samuelson who is not a proponent of propertization, claims that "information privacy goals may not be achievable unless the default rule of the new property rights regime limits transferability."[184] Most market proponents, however, favour the default rules that can be "bargained around."[185]

Kang recognizes that merely deciding on the initial entitlement in personal data is insufficient and, compared to Murphy's privacy versus disclosure dichotomy, develops a more elaborated system of the default rules. Since it is not efficient for individuals to have to research what information about them is collected and how it is used a contractual default rule should be adopted that "personal information may be processed in only functionally necessary ways" and that parties are "free to contract around the default rule."[186] The ban on transfer on personal data from the individuals, or inalienability rules in Kang's view would be too paternalistic. "Control is at the heart of information privacy," he claims, and control means that individuals should be able to sell or disclose their information if they wish so.[187] Inalienability will risk "surrendering control over information privacy to the state."[188] According to Solove, Kang's solution "creates a property right in personal information through a contractual default rule that limits the way personal information is used after being transferred to another."[189]

Paul Schwartz offers probably the most elaborated, and more intrusive, set of the default rules, or better, a model of the property regime for data protection. He tries to account for three elements of critique of propertization in his hybrid inalienability model, those elements being "public good" nature of information privacy; the market failures, i.e. pointing to the impact of propertization under current conditions; and resentment to free alienability of personal data which implies that the owner of it may sell it whenever he pleases on whatever conditions.[190] First, he asserts that a public good argument which reads that market cannot possibly account for a social value of privacy, does not reject propertization entirely but calls for restrictions on it. As examples of the privatized public goods he names outsourcing in some sectors of national defence, marketization of environmental laws, and democratic discourse via private media.[191] The market failures, he argues, may be corrected via regulation which constitutes a part of his model.[192] As for the fear of unrestricted alienability,

---

182 DJ Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. R. 1393, , p. 1448

183 Ibid.,

184 P Samuelson, "Privacy as Intellectual Property?" (2000) 52 Stan. L. R. 1125,

185 DJ Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. R. 1393,

186 J Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stan. L. R. 1193,

187 Ibid.,

188 Ibid.,

189 DJ Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. R. 1393,

190 PM Schwartz, "Property, Privacy, and Personal Data" (2004) 117 Harv. L. Rev. 7 2055, , p. 2076

191 Ibid., p. 2090

192 Ibid., p. 2089

Schwartz submits that free alienability is not implied by his model since "[according to Blackstone,] property can also take the form of incomplete interests [i.e. be inalienable – N.P.] and [...] can serve to structure social relationships."[193] This is a premise on which the copyright law[194] and the US intellectual property jurisprudence rely when rejecting the exclusivity axiom.[195] The hybrid inalienability model that arguably responds to all three challenges thus implies: "limitations on the individual's right to alienate personal information; default rules that force disclosure of the terms of trade; a right of exit for participants in the market; the establishment of damages to deter market abuses; and institutions to police the personal information market and punish privacy violations."[196] The default rules are: an allowed initial transfer of personal data from the individual, but only if the individual has an opportunity to stop further transfers or uses by third parties. The ability to block is to be set as an opt-in, that is, any further use or transfer is not allowed without an affirmative consent.[197]

The model proposed by Schwartz is probably the most privacy-friendly among the ones outlined here. However, one may ask what is left of the idea of propertization when property rights are so heavily regulated, and why then not to opt for mere regulation. The point of a special interest is Schwartz's rejection of the "exclusivity axiom." It has been shown that it lies at the core of the utilitarian argument for propertization. By rejecting it, Schwartz's model is not able to perform any 'market' functions imposed on property by e.g. more economically oriented points of view. Thus, the only value of calling the set of rights vis-à-vis personal data in Schwartz's model is that using the label of property will overcome structural limitations of the US legal system, e.g. by changing the balance between privacy and the free speech considerations in tort and constitutional cases, as well as, property law being mostly judge-made, avoid the necessity to push new legislation through the US Congress.

To sum up, the lesson Europeans can learn from the US debate on default rules is that property is not an entirely straightforward concept. It has many faces and bears more than one function, among others, facilitating market exchange (function of property used by utilitarian views and better achieved with minimal regulation) or a mere protective function (performed by invoking other than market qualities of property). Therefore, the answer to the question whether or not propertization of personal information might be a good idea for Europe cannot be simply yes or no, but requires further deliberations on what approach to data protection – market or non-market - we are prepared to take, what 'face' of property suits best for it, and, most intriguingly, if the approach is non-market, do we have to go through the trouble of introducing a new model of data protection via property, like Americans, possibly, do.

3.4 Critique of propertization

Despite a seeming popularity of the idea, a number of the US commentators are opposed to propertization of personal information. Mainly, the criticism is aimed at the 'market face' of property. As explained earlier, Paul Schwartz distinguishes three traditional elements of critique of propertization of personal data: "public good" nature of information privacy; related to the market failures, i.e. pointing to the impact of propertization under current conditions; and resentment of free alienability of personal data.[198]

A number of the commentators see commodification (and propertization as a legitimized commodification) of certain goods including personal data as a problem. This is a "public

193 PM Schwartz, "Property, Privacy, and Personal Data" (2004) 117 Harv. L. Rev. 7 2055, Ibid., p. 2092
194 Ibid., p. 2093
195 Ibid., p. 2093
196 Ibid.
197 Ibid., p. 2060
198 Schwartz 2004, p. 2076

good" argument which implies that information privacy has not only individual but wider social value. The market cannot account for the latter. According to Katrin Schatz Byford, treating "privacy as an item of trade [...] values privacy only to the extent it is considered to be of personal worth by the individual who claims it."[199] For Pamela Samuelson, propertization of privacy as a civil liberty might be "morally obnoxious."[200] The access to privacy, as to clean air, "should not depend on socioeconomic status."[201]

Peter Swire challenges market solutions on the ground of the failures of the currently existing information market. Even if propertization will enable individuals to negotiate their privacy, consumers have no expertise in privacy issues and bargaining costs time and effort.[202] So negotiating with corporations will remain difficult. The introduction of PETs may save the time and effort. However, whether it will substitute the needed expertise is questionable. Other failures of the current information markets are asymmetric information available to data collectors and individuals, and "bounded rationality" of consumers.[203]

The argument *against* propertization aimed at the core of the utilitarian argument is made by Jessica Litman. She disputes understanding of property explained by Calabresi and Melamed, i.e. as protecting the entitlement and preventing the transfer of information other than within a voluntary transaction. She refers to the legal definition of property given in the Restatement[204] and says that "the raison d'être of property is alienability; the purpose of property laws is [not to prevent but to encourage and – N.P.] [...] prescribe the conditions for transfer."[205] Litman argues that the regulation takes the property model for intangible interests, like intellectual property, when it aims "to make it easy to sell them."[206] That being said, the control which propertization is argued to be able to achieve, defined as a "right to exclude" others, is of the same kind as control conferred by already existing torts: battery protects the integrity of the body, defamation protects the reputation without defining them as property. It is similarly unnecessary to treat information privacy as property merely to protect it from invasion.[207]

Litman also challenges Lessig's proposal to use property as an instrument to promote investments in PETs. She labels Lessig's argument "a fairy-tale picture" since industries do not respect information privacy because it is expensive to honour privacy preferences, not to express them.[208] Litman expresses her disbelief in market solutions since "the market in personal data is the *problem*. Market solutions [...] won't cure it; they'll only legitimize it."[209]

Criticism of the propertization by Solove combines market and non-market arguments. To understand Solove's standpoint, one should recall that his definition of the data protection problem goes beyond privacy as control. Solove argues that privacy-friendly propertization solutions fail to resolve the information privacy problem because they do not address its substance, i.e. "the power inequalities [...] between individuals and bureaucracies."[210] It is problematic for an individual to adequately value specific personal information because this

---

199 K Schatz Byford, "Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment" (1998) 24 Rutgers Computer & Tech. L.J. 1,

200 Samuelson 2000, p. 1143

201 Schwartz 2004, p. 2086

202 PP Swire, "Markets, Self-regulation, and Government Enforcement in the protection of personal information" http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472, p. 10 (accessed on November 18th 2008)

203 Schwartz 2004, p. 2081

204 Restatement of Property, §489 cmt. a (1944)

205 Litman, p. 1295

206 Ibid, p. 1296

207 Litman, p. 1296

208 Ibid., p. 1297

209 Ibid., p. 1301

210 Solove 2001, p. 1452

value is tied up to yet unknown future uses.[211] However, the problem is not the inability of an individual to put a price tag on information, but an aggregated inability of many individuals disempowering them in the information society.[212]

To sum up, a European reader can benefit from several points following from the criticism of the US propertization proposals. First, to confirm the point made in the previous section, the American debate disregards the fact that property is perceived and, in fact, functions in different ways. Main criticism is aimed at the 'market face' of property legitimizing to a larger or lesser extent commodification of personal information. Schwartz's hybrid inalienability model, however, meets no criticism at all. That suggests that in deciding for or against propertization, also in Europe, a lot depends not on the standpoint taken towards propertization on its face, but towards the phenomenon of commodification.

Second, in advocating as well as criticising the idea of property rights in personal data, some empirical statements have been made and left without support of any empirical study. One kind of such statements is related to the nature of the problem with personal data and its processing. Since the nature of the problem in principle defines the tools to tackle it, Europeans should look more into the substance of that matter, also in empirical studies. Another empirical statement is related to the role of property in restoring control over personal data. Who is right: Lessig who claims, first, that the use of the term 'property' alone will make people more aware of the value of privacy, and, second, that property will be an engine bringing a better mechanism of data protection into action, or Litman, insisting that one cannot fight undesirable data market by market tools – has to be a subject of a sociological study.

4. Conclusions: Lessons for Europe

To sum up, although due to specificities of the US legal and political system Europeans cannot fully embrace the results of the American debate on propertization of personal data, there are quite some lessons to learn from it. The first, and by far, the most important lesson is that the concept of property has more than just one face. The US debate mostly overlooks this fact, but a European discussion should take into account that introduction of property rights may serve both market and non-market, or protective function. In the US the latter has received expression in the proposals to introduce property rights in data but limit alienability (the scope of property rights in general) in order to avoid the limitations of the current legal and political system. From that the European reader should learn to be open to consider property out of the 'market box', too.

Second, whether property may be invoked in its market or non-market face depends on a function policy-makers choose for it to perform. Market face, for instance, will be a good tool to implement Lessig's theory and create a system where property creates incentives for better data protection and, arguably, gives individuals control over their data back. Non-market face, characterized by limited scope of property rights, is suitable for implementing the idea of rhetoric value of propertization. It is also possible to assume that in Europe introduction of property rights in an object does not have to mean that a free market in that object is legitimized. On the contrary, free alienability excluded, property may as well be valued for its protective function.

Third, before the choice for or against propertization of personal data is made, Europe has to decide on a number of other fundamental issues. An important one is what its standpoint is vis-à-vis commodification of personal information, whether, in principle, it opposes market

---

211 Ibid., p. 1452

212 Ibid., p. 1453

exchange of personal data or ready to go along with it, albeit, in a (more or less) restricted form. The answer to this question, in turn, largely depends on the chosen regulatory strategy and priorities and the vision of the role of the state or supranational institutions (paternalistic versus liberal).

The fourth lesson for Europe is that to shape their view on commodification and propertization of personal data, Europe has to come to a uniform understanding of the essence of the problem it attempts to tackle (if any). In the American literature propertization is called upon to resolve the problem of the lost control over personal information. But does Europe want its citizens to have full control over a last bit of information pertaining to them? Another function propertization, albeit in theory, serves in the US debate is a 'back-door' introduction of data processing regulation, since a straightforward way at times is problematic. It is unlikely that Europe experiences same difficulties introducing new regulations. However, possibly there is something more to that protective function of property that Europe can also use. The first thing which comes to one's mind is that status of property rights may give data protection rights an extra set of enforcement mechanisms, but that is a subject of further research.

Finally, coming back to the first lesson, Europeans should decide on what scope of rights they prefer with regard to personal data, and then see if they have to label those 'property' or, probably, not.

Nadezhda Purtova *(N.Purtova@uvt.nl) Ph.D candidate at TILT, Tilburg Institute for Law, Technology, and Society, The Netherlands*