Scientific Research Publishing

Open Journal of Philosophy, 2018, 8, 206-215
http://www.scirp.org/journal/ojpp
ISSN Online: 2163-9442
ISSN Print: 2163-9434

Personal Data v. Big Data: Challenges of Commodification of Personal Data

Maria Bottis, George Bouchagiar

Ionian University, Corfu, Greece
Email: botti@otenet.gr, georgebouchayar@yahoo.gr

How to cite this paper: Bottis, M., & Bouchagiar, G. (2018). *Personal Data v. Big Data*: Challenges of Commodification of Personal Data. *Open Journal of Philosophy, 8,* 206-215.
https://doi.org/10.4236/ojpp.2018.83015

Received: March 22, 2018
Accepted: May 8, 2018
Published: May 11, 2018

Copyright © 2018 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

Any firm today may, at little or no cost, build its own infrastructure to process personal data for commercial, economic, political, technological or any other purposes. Society has, therefore, turned into a privacy-unfriendly environment. The processing of personal data is essential for multiple economically and socially useful purposes, such as health care, education or terrorism prevention. But firms view personal data as a commodity, as a valuable asset, and heavily invest in processing for private gains. This article studies the potential to subject personal data to trade secret rules, so as to ensure the users' control over their data without limiting the data's free movement, and examines some positive scenarios of attributing commercial value to personal data.

Keywords

Personal Data, Commodification, Trade Secret

1. Introduction

Despite the European legislator's latest efforts to protect both natural persons, with regard to the processing of personal data (meaning any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, see Article 4(1) of the GDPR), and free movement of such data, private businesses not only massively process (collect, organize, alter, disclose, combine, erase or destroy) personal data (Pasquale, 2015: p. 56), but also view the latter as an asset (Almunia, 2012; Cohen, 2000: p. 1375; O'Neil, 2016: p. 151; Prins, 2006: p. 228; Hoofnagle, 2003; Michaels, 2008) and, thus, sell it, exchange it or even produce it (Crawford & Schultz, 2014: pp. 94-95, 98; Prins, 2006: pp. 226-230). Scholars speak of theft of humanistic property (Mann, 2000) and argue that natural persons should get paid for such processing (Laudon, 1996: p. 103). Users by a "single

mouse-click" give their valid consent (Recital (32) of the GDPR) to the processing of their sensitive information. Some authors worry that algorithms discriminate against consumers, when projecting the "perfect ad" (A29DPWP, 2013: p. 46), promoting the "appropriate good" at the "appropriate price" (Turow & McGuigan, 2014: pp. 27-29; EDPS, 2015: p. 19), predicting criminal behaviors (Chander, 2017: p. 1026) or "evaluating" the accused before sentencing courts (*State v. Loomis*, 2016).

Such practices reveal a need to regain the users' control over their personal data. This paper briefly examines the potential to subject personal data to trade secret protection rules and studies the outcome of attributing commercial value to such data.

2. Regaining Control by Subjecting Personal Data to Trade Secret Rules

If personal data were treated as trade secrets, it seems that the data subjects would better control their private information without limiting the free movement of this data (Prins, 2004; Malgieri, 2017). Personal data could be protected by rules that govern trade secrets (Samuelson, 2000), which ensure such control that enables that the secret holder not only keeps private information well-hidden, but also benefits from its exploitation (Franzoni & Kaushik, 2016).

Trade secrets, or know-how (*i.e.* a package of (non-patented) practical information, resulting from experience and testing by the franchisor, which is secret, substantial and identified, see Article 1(3)(f) of Commission Regulation (EEC) No 4087/88; Article 1(1)(i) of Commission Regulation (EC) No 772/2004), are separately protected in the law and differ from industrial property rights, copyright and neighboring rights (Article 1(1)(g) of Commission Regulation (EC) No 772/2004). Under Article 2(1)(a-c) of Directive (EU) 2016/943 of the European Parliament and of the Council (hereinafter referred to as "Directive (EU) 2016/943"), "trade secret" means information which is secret (in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question, see Article 2(1)(a) of Directive (EU) 2016/943), has commercial value because it is secret, and has been subject to reasonable—under the circumstances—steps, by the person lawfully in control of the information, to keep it secret. Thus, each "item of information" may be protected as a trade secret, given that the latter extends to the commercial data, such as information on customers and suppliers (Recital (2) of Directive (EU) 2016/943). Moreover, with regard to its legal status, right to know-how, in contrast with other intellectual property rights, does not constitute an absolute right (Lemley, 2008: p. 330). It is a stand-alone legal right capable of being separately protected. In addition, a trade secret right is not exclusive (Recital (16) of Directive (EU) 2016/943).

Under Directive (EU) 2016/943, the acquisition of a trade secret without the consent of the trade secret holder shall be considered unlawful, whenever carried

out by unauthorized access to, appropriation of, or copying of "data" (e.g. documents, objects, or electronic files), lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced (Article 4(2)(a) of Directive (EU) 2016/943). The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person who is found to have acquired the trade secret unlawfully or has been in breach of a confidentiality agreement or any other duty not to disclose the trade secret or has been in breach of a contractual or any other duty to limit the use of the trade secret (Article 4(3) of Directive (EU) 2016/943). The acquisition, or use or disclosure, of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition (or use or disclosure), knew or ought, under the circumstances, to have known that the trade secret had been obtained unlawfully (Article 4(4) of Directive (EU) 2016/943).

Given the above, one can conclude that when a person, a licensor, has provided "data", which constitute trade secrets, to another for a particular purpose, these data cannot be used for other purposes without obtaining the licensor's permission. At the same time, license rights may be lawfully further transferred by the licensee, only if such right to sublicense has been agreed, *i.e.* only if the initial licensor has given her consent. Indeed, the above conclusions constitute general rules that govern trade secrecy at international level (Samuelson, 2000: pp. 1155-1156; Byrne, 1998: pp. 210-211; McDaniel, 1986: pp. 45-47).

Can personal data fulfill the trade secret's definition? Personal data, which a private company has collected, are admittedly not generally known amongst or readily available to other businesses that collect data. An ID number, which a company that provides, for example, accommodation services has collected, is not generally known among other businesses nor is readily accessible to such enterprises (of course, under its privacy policy, an enterprise may share one's ID number with other private companies, but we will consider here that this ID number is "secret" within the meaning of Article 2(1)(a) of Directive (EU) 2016/943). In addition, personal data do have commercial value exactly because they are generally secret. Moreover, the person lawfully in control of personal data, *i.e.* a private company which collects personal data, takes or should take reasonable steps to keep the data secret, as demanded by the law and as generally the companies claim (O'Donoghue, 2017). Finally, the right to the protection of personal data may be fundamental (Article 8 of CFREU), but it is certainly not an absolute right (Recital (4) of GDPR), exactly as the right to a trade secret. It appears, then, that under certain conditions, personal data can be trade secrets as well.

If it were accepted that personal data, under certain conditions, fulfill the trade secret's definition, the treatment of the right to personal data as a right to a *quasi* (Malgieri, 2017), at least, trade secret could guarantee adequate consumer protection. Besides, one could claim that personal data ought to be secret, in the sense that it ought not to be generally known among or readily accessible to

persons within the circles that normally deal with the kind of information in question. Moreover, given that personal data possibly subject to exploitation, it ought to have commercial value, because it is secret by default, at least in Europe. A private company, which is lawfully in control of personal data, is by law obliged to take reasonable measures to keep its personal data secret. Hence, given contemporary reality, personal data "ought to" simultaneously fulfill trade secret's definition. If licensing rules that govern trade secrets were applied to personal data processing, consumers, as licensors, would provide data to businesses for a particular purpose. Thus, it would be prohibited to use such data for other purposes without the licensor's permission or to further transfer license rights without the initial licensor's consent (Hon, Millard, & Walden, 2012).

Under rules that govern trade secrets, confidentiality and, thus, trade secret rights, should be used as a tool for business competitiveness and innovation management (Article 5(1)(f), Recitals (39), (49) and (83) of GDPR; Recital (2) of Directive (EU) 2016/943). Hence, if personal data were treated as *quasi* trade secrets, a dynamic competition would very likely take place. In this context, perhaps stronger guarantees could be provided, in particular with regard to the transparency of the processing of personal data. Perhaps we would see new, high-quality services to the end user and initial licensor. Private companies, which would be unable to further transfer personal data to third parties without the licensor's permission, would likely endorse new technologies to transparently and rationally process personal data for specific purposes, which would have, in any case, been determined by the licensor (Samuelson, 2000).

3. Positive Scenarios of Attributing Commercial Value to Personal Data

If personal data were governed by trade rules, individuals would likely be more aware of their own information's value and power. This awareness should be considered to be an essential prerequisite that would enable persons to control their data.

An individual may enjoy a specific service, such as, for instance, a free e-mail service, having given her consent to the processing of her data. The company supplying the email service processes the user's data in multiple ways (by collecting it, analyzing it, correlating it etc.). Even if the user has freely given her consent to this processing, a case in which "too much mouse-clicking" would be required (Recital (43) of GDPR), the e-mail service provided remains "one and single". Thus, one should wonder whether this one service "costs" or should cost that much as is worth the fee against which it is offered. The fee is or should be equal not to the value of a single data processing operation but to the value of unlimited, in multiple ways and perpetual further processing of personal data.

Could commercial value be attributed to personal data to enable the individual to realize, after having been aware of this value (Prince, 2018: p. 22; Malgieri & Custers, 2017), the "heavy costs" she pays for "free" digital services?

International institutions have recognized that personal data may be provided

or used as money in exchange for the supply of digital content and digital services (Article 3(1) of Proposal of the European Commission, 2015; Report of the European Parliament, 2017). At the same time, sensitive items of information tend to become or have—in practice—already become the new currency of the Internet age. Given countless services and huge volume of content, which are, on a daily basis, supplied to the consumer, in exchange for which personal data are provided, the consumer's data undeniably have some non-negligible economic value, the exact calculation of which has already become subject to scientific investigations (OECD, 2013; Chirita, 2018: p. 11; EDPS, 2014: p. 9).

As some scholars argue, personal data that concern some general attributes, such as age, "is worth less" than other, more sensitive, personal information e.g. data concerning health, which are "worth about 26 cents per person" (Malgieri & Custers, 2017: p. 6). The value of the information "George drinks chocolate at home" must be lower than the value of the information "every Saturday at 09.00 a.m. George and his girlfriend, named Stella, drink chocolate at George's apartment (31 rue Dedieu 987776 Villeurbanne), whilst listening to jazz". Although under some studies or some "personal data's value calculators" (Steel, Locke, Cadman & Freese, 2013; Curtis, 2015; BCG, 2012), the total value of all this information may be less than a "dollar per person and peruse", each person provides her data constantly and on a daily basis. An individual may provide same personal data (e.g. an e-mail or a last name) to multiple companies, whereas each enterprise need only collect data from each person once. Furthermore, numerous correlations of data, which are promoted by Big Data technologies, may attribute "higher value" to the same data, given that they may be combined in multiple ways.

So personal data have economic value, which is in fact countable. There would be nothing unreasonable, it follows, in adopting rules, which would enable individuals to know the value of their data and, thus, to better control processing (Malgieri & Custers, 2017: p. 10).

For example, if a user knew that total value of her personal data, collected, analyzed, correlated or transferred from and to multiple businesses within a month, was EUR 200, then she would probably change her views on processing. Users might realize that any company is indeed "literally dependent" on natural persons giving their consent to the processing of their data. Perhaps it is not always the user who needs an enterprise that supplies, for example, "search on the web" services, but the other way round. As a result, a possible "mass-refusal" to tick the box and accept a business's terms of use and privacy policy and, thus, services would harm the company. As enterprises while supplying free services ask for the completion of certain "standard" data fields (for the sake of brevity, let these be: name with "value" X euro, last name with "value" Y euro and e-mail with "value" Z euro), users would become aware that for any service supplied, the fee is the same for one person (X + Y + Z euro), but it may be different for each individual (EDPS, 2015). This, in conjunction with transparent data processing, would enable the consumer to know the way he is being sorted and

the very fact of the charging (on the basis of this sorting) of different prices for same service. Consumers' awareness of the way they are being categorized is the key-element on which fairness (and lawfulness) of price discrimination depends (Hildebrandt, 2007; Steppe, 2017: p. 781).

All these "scenarios", cited above as examples, which could be the outcome of a possible subjection of personal data to trade rules, would enable persons to better control the processing of their personal data. At the same time, free movement of the latter would be ensured and, thus, personal data would be transparently processed for the benefit of humanity and science.

4. Conclusion

To subject personal data to trade rules might help further resolve other crucial issues, such as that of the processing personal data of the deceased. Provisions on the protection of natural persons with regard to the processing of personal data do not apply to the personal data of deceased persons (Recitals (27), (158) and (160) of GDPR). Hence, any enterprise may, unconditionally, without consent and for any purpose it may wish, process a huge volume of personal data of subjects/users, who passed away, after having "ticked too many boxes" during their lifetime (Bouc, Han, & Pennington, 2016: p. 636).

If personal data have economic value, perhaps we should consider negative that this value should end up in private companies, which were or are collecting them, while the subject was, or is alive, and which will perpetually continue to process them and exploit them for profit in multiple ways. This should perhaps be deemed negative, not so much because of an unjustifiable economic benefit which private enterprises earn, but because perhaps some of this value of personal data should, as a matter of justice, probably reach the subject's heirs. This is because these are the "loved ones" and the only persons with whom in the offline environment the subject shared and to whom she trusted her personal information that concerned her health, her personal conversations, or even, the fact that she "went for a walk" somewhere sometime during her lifetime. The individuals should have the right not to let these items of information, which may now "by a single mouse-click be turned" to private companies, become after their death private companies' perpetual source of income. Besides, given that personal data commercialization would enable the former to be transferred as assets, some significant social problems could be resolved, such as that of lack of financial resources in the area of some non-profit institutions that pursue vital e.g. social, educational or cultural objectives and which the data subject might wish to include in her will.

Setting aside personal data of deceased persons and focusing on those of the living ones, we should question whether the use of potential future personal data with commercial value, which any individual could produce just by living her life, could help resolve some even more important global issues, such as poverty, given that every person could, perhaps, earn some financial benefit in exchange

of her data.

In the past, when it was asked "What would people do when they no longer needed to grow food to survive?", the answer was given by the industrial revolution (Lemley, 2015: p. 513; Overton, 1996). In an age of abundance and a world without scarcity (Lemley, 2015: p. 514; Rotman, 2013), humanity could be directed towards new exchange models, where people would be rewarded for their acts of benevolence and contribution to societies. Individuals might just find new things to do or they would devote their time to the creation and production of knowledge, just because there would be time to be devoted to such purposes. Optimistic scenarios are countless and perhaps preferable, for example, to the opaque processing of personal data in favor of private businesses' interests, without the knowledge of the data-subject and, sometimes, through discriminatory procedures.

References

A29DPWP (2013). *Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation*.
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

Almunia, J. (2012). *Speech (Nov. 26, 2012) "Competition and Personal Data Protection"*.
http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm

BCG (Boston Consulting Group) (2012). *The Value of Our Digital Identity*. USA: Liberty Global, Inc.
http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

Bouc, A., Han, S.-H., & Pennington, N. (2016). "Why Are They Commenting on His Page?": Using Facebook Profile Pages to Continue Connections with the Deceased. *Computers in Human Behavior, 62,* 635-643. https://doi.org/10.1016/j.chb.2016.04.027
https://www.sciencedirect.com/science/article/pii/S0747563216303028

Byrne, N. (1998). *Licensing Technology* (2nd ed.). Bristol: Jordan Pub.

CFREU (2000). Charter of Fundamental Rights of the European Union. 18.12.2000 Official Journal of the European Communities C 364/1.
http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Chander, A. (2017). The Racist Algorithm? *Michigan Law Review, 115,* 1023-1045.
https://repository.law.umich.edu/mlr/vol115/iss6/13/

Chirita, A. D. (2018). The Rise of Big Data and the Loss of Privacy. In Bakhoum, Gallego Conde, Mackenordt & Surblyte (Eds.), *Personal Data in Competition, Consumer Protection and IP Law—Towards a Holistic Approach?* Berlin: Springer.
https://ssrn.com/abstract=2795992
http://dx.doi.org/10.2139/ssrn.2795992

Cohen, J. (2000). Examined Lives: Informational Privacy and the Subject as Object. *52 Stan. L. Rev.*, 1373-1438.
https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub

Commission Regulation (EC) No 772/2004. Commission Regulation (EC) No 772/2004 of 27 April 2004 on the Application of Article 81(3) of the Treaty to Categories of Technology Transfer Agreements.

Commission Regulation (EEC) No 4087/88. Commission Regulation (EEC) No 4087/88 of 30 November 1988 on the Application of Article 85 (3) of the Treaty to Categories of Franchise Agreements.

Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review, 55,* 93-128. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784

Curtis, S. (2015). *How Much Is Your Personal Data Worth? The Average Consumer Values Their Personal Data at £3,241, According to New Research*. Telegraph. http://www.telegraph.co.uk/technology/news/12012191/How-much-is-your-personal-data-worth.html

Directive (EU) 2016/943. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) against Their Unlawful Acquisition, Use and Disclosure.

EDPS (2014). *Preliminary Opinion of the European Data Protection Supervisor, Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy*.

EDPS (2015). *European Data Protection Supervisor, Opinion 7/2015, Meeting the Challenges of Big Data—A Call for Transparency, User Control, Data Protection by Design and Accountability*.

Franzoni, L. A., & Kaushik, A. K. (2016). The Optimal Scope of Trade Secrets Law. *International Review of Law and Economics, 45,* 45-53. https://www.sciencedirect.com/science/article/pii/S0144818815000708 https://doi.org/10.1016/j.irle.2015.11.004

GDPR (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*.

Hildebrandt, M. (2007). *Profiling into the Future: An Assessment of Profiling Technologies in the Context of Ambient Intelligence*. https://www.researchgate.net/publication/242576589_Profiling_into_the_future_An_assessment_of_profiling_technologies_in_the_context_of_Ambient_Intelligence

Hon, W. K., Millard, C., & Walden, I. (2012). Who Is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2. *International Data Privacy Law, 2,* 3-18. https://ssrn.com/abstract=1794130

Hoofnagle, C. J. (2003). Big Brother's Little Helpers: How Choice Point and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement. *North Carolina Journal of International Law and Commercial Regulation, 29,* 595-638. https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1677&context=facpubs

Laudon, J. C. (1996). Markets and Privacy. *Communications of the ACM, 39,* 92-104. https://dl.acm.org/citation.cfm?id=234476 https://doi.org/10.1145/234215.234476

Lemley, M. A. (2008). The Surprising Virtues of Treating Trade Secrets as IP Rights. *Stanford Law Review, 61,* 311-354. http://heinonline.org/HOL/Page?handle=hein.journals/stflr61&div=12&id=&page=&collection=journals

Lemley, M. A. (2015). IP in a World without Scarcity. *New York University Law Review, 90,* 460-515. http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-90-2-Lemley.pdf

Malgieri, G. (2017). Quasi-Property in Consumer Information: Trade Secrets and Consumer Rights in the Age of Big Personal Data. In M. Bottis, & E. Alexandropoulou (Eds.), *Proceedings of the 7th International Conference on Information Law and Ethics, ICIL 2016, Broadening the Horizons of Information Law and Ethics. A Time for Inclusion* (pp. 376-400). Thessaloniki: University of Macedonia Press. https://icil.gr/2016/icil/proceedings/

Malgieri, G., & Custers, B. (2017). Pricing Privacy—The Right to Know the Value of Your Personal Data. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34,* 289-303. https://www.sciencedirect.com/science/article/pii/S0267364917302819

Mann, S. (2000). Computer Architectures for Protection of Personal Informatic Property: Putting Pirates, Pigs, and Rapists in Perspective. *First Monday, 5*. http://firstmonday.org/ojs/index.php/fm/issue/view/121 https://doi.org/10.5210/fm.v5i7.774

McDaniel, T. B. (1986). Shop Rights, Rights in Copyrights, Supersession of Prior Agreements, Modification of Agreement, Right of Assignment and Other Contracts. *AIPLA Quarterly Journal, 35,* 45-47. http://heinonline.org/HOL/Page?handle=hein.journals/aiplaqj14&div=11&g_sent=1&casa_token=&collection=journals

Michaels, J. D. (2008). All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror. *California Law Review, 96,* 901-966. https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1169&context=californialawreview

O'Donoghue, C. (2017). *UK: Spanish DPA Fines Facebook €1.2 Million for Data Protection Infringements*. http://www.mondaq.com/article.asp?articleid=632558&email_access=on&chk=2169390&q=1536832

O'Neil, C. (2016). *Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy*. New York, NY: Broadway Books.

OECD (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*. OECD Digital Economy Papers, No. 220, Paris: OECD Publishing. https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en

Overton, M. (1996). The Agricultural Revolution Reconsidered. In *Agricultural Revolution in England: The Transformation of the Agrarian Economy 1500-1850* (pp. 193-207). Cambridge Studies in Historical Geography, Cambridge, MA: Cambridge University Press. https://doi.org/10.1017/CBO9780511607967.007

Pasquale, F. (2015). *The Black Box Society, the Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press. https://doi.org/10.4159/harvard.9780674736061

Prince, C. (2018). Do Consumers Want to Control Their Personal Data? Empirical Evidence. *International Journal of Human-Computer Studies, 110,* 21-32. https://www.sciencedirect.com/science/article/pii/S1071581917301416 https://doi.org/10.1016/j.ijhcs.2017.10.003

Prins, C. (2006). Property and Privacy: European Perspectives and the Commodification of Our Identity. In L. Guibault, & B. Hugenholtz (Eds.), *The Future of the Public Domain, Identifying the Commons in Information Law* (pp. 223-258). Alphen aan den Rijn: Kluwer Law International.

Prins, J. E. J. (2004). The Propertization of Personal Data and Identities. *Electronic Journal of Comparative Law, 8,* 1-7. https://www.ejcl.org/83/art83-1.PDF

Proposal of the European Commission (2015). *Proposal of the European Commission for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content.*

Report of the European Parliament (2017). *Report of the European Parliament on the Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content.* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA8-2017-0375%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN

Rotman, D. (2013). *How Technology Is Destroying Jobs.* https://www.technologyreview.com/s/515926/how-technology-is-destroying-jobs/

Samuelson, P. (2000). Privacy as Intellectual Property? *Stanford Law Review, 52,* 1125-1173. https://scholarship.law.berkeley.edu/facpubs/2137/ https://doi.org/10.2307/1229511

State v. Loomis (2016). *881 N.W.2d 749 (Wis. 2016).* https://harvardlawreview.org/2017/03/state-v-loomis/

Steel, E., Locke, C., Cadman, E., & Freese, B. (2013). *How Much Is Your Personal Data Worth? Use Our Calculator to Check How Much Multibillion-Dollar Data Broker Industry Might Pay for Your Personal Data.* Financial Times. http://ig.ft.com/how-much-is-your-personal-data-worth/

Steppe, R. (2017). Online Price Discrimination and Personal Data: A General Data Protection Regulation Perspective. *Computer Law & Security Review, 33,* 768-785. https://www.sciencedirect.com/science/article/pii/S0267364917301656 https://doi.org/10.1016/j.clsr.2017.05.008

Turow, J., & McGuigan, L. (2014). Retailing and Social Discrimination: The New Normal? In S. P. Gangadharan (Ed.), *Data and Discrimination: Collected Essays* (pp. 27-29). Open Technology Institute. https://na-production.s3.amazonaws.com/documents/data-and-discrimination.pdf