Open Journal of Philosophy, 2018, 8, 192-205
http://www.scirp.org/journal/ojpp
ISSN Online: 2163-9442
ISSN Print: 2163-9434

Personal Data v. Big Data in the EU: Control Lost, Discrimination Found

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* in the EU: Control Lost, Discrimination Found. *Open Journal of Philosophy, 8,* 192-205
https://doi.org/10.4236/ojpp.2018.83014

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

Abstract

We live in the Big Data age. Firms process an enormous amount of raw, unstructured and personal data derived from innumerous sources. Users consent to this processing by ticking boxes when using movable or immovable devices and things. The users' control over the processing of their data appears today mostly lost. As algorithms sort people into groups for various causes, both legitimate and illegitimate, fundamental rights are endangered. This article examines the lawfulness of the data subject's consent to the processing of their data under the new EU General Data Protection Regulation. It also explores the possible inability to fully anonymize personal data and provides an overview of specific "private networks of knowledge", which firms may construct, in violation of people's fundamental rights to data protection and to non-discrimination. As the Big Data age is here to stay, both law and technology must together reinforce, in the future, the beneficent use of Big Data, to promote the public good, but also, people's control on their personal data, the foundation of their individual right to privacy.

Keywords

Personal Data, Consent, Control, Discrimination

1. Introduction

In the age of Big Data (King & Forder, 2016: p. 698; Giannakaki, 2014: p. 262), information (Lessig, 2006: pp. 180-185; Summers & DeLong, 2001) fully confirms its etymological origin (Araka, Koutras, & Makridou, 2014: pp. 398-399) and becomes abundantly available (Himma, 2007). It constitutes a mass-produced good (Battelle, 2005), consumed as a commodity, rather than leveraged as a tool for personal growth of the individual or the development of democratic societies (Koelman, 2006). Information, including personal data (i.e. "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 GDPR), has acquired independent economic value (Pasquale, 2015: p. 141; Hugenholtz & Guibault, 2006) and, thus, new and innovative business models constantly emerge and dominate the market. For instance, a business that owns no vehicles (such as Uber) may dominate the "taxi market", while large "hoteliers" (e.g. Airbnb) may own no property at all (Chesterman, 2017). Firms, thus, process raw (Giannakaki, 2014), unstructured (Mayer-Schönberger & Cukier, 2013: p. 47) and personal (Picker, 2008; Tene, 2008) data (Scholz, 2017: pp. 9-12) from a multiplicity of sources (Tene, 2011). The Internet of Things (Panagopoulou-Koutnatzi, 2015a) only dramatically accentuates the huge potential of these vast collections of information (Petrovic, 2017: p. 187).

How do firms obtain data from people? A way to extract them is a peculiar quid pro quo: Data constitute the "fee" that users "pay" for multiple "free" digital services. This "deal" has not only been accepted by a number of institutions (European Commission, 2017), but has also become both a global phenomenon and an everyday business practice. While providing a service, e.g. an e-mail service, a firm can collect and process personal information contained in the e-mail (Prins, 2006: p. 229). Data collected may also concern e.g. the language the user speaks or her mobile phone or her real location (or even device-specific information, such as hardware model, operating system version, unique device identifiers and mobile network information). In addition, when a user stores her digital, and sometimes personal, files using Cloud Computing (for instance, Dropbox, Google Drive, Sky Drive, i-Cloud), the provider, i.e. the company that offers the cloud service, may process data contained in the user's (Lidstone, 2014) files stored in the "clouds" (Morozov, 2011: p. 286). Finally, a cornucopia of data that relate to a user's health, movement or just living patterns (e.g. heart rate, blood pressure, or even sleep times) may be collected and processed as long as users, accompanied by smart devices (Brabazon, 2015) and selecting from innumerous applications (Mayer-Schönberger & Cukier, 2013: p. 94), measure themselves during their everyday physical activities.

Thus, countless online activities, a standard feature of everyday life, involve the production and the processing (Tene & Polonetsky, 2013: p. 255) of an unprecedented volume of personal data (Committee on Commerce, Science, and Transportation, 2013). Although it is doubtful whether someone's recorded heart rate constitutes personal data, many, or perhaps most of the kinds of information described above as examples are, actually, personal data under the General Data Protection Regulation of the EU. This is because in the age of Big Data, the collection of a huge volume of data enables firms to draw numerous conclusions that relate to one person and makes it possible to identify a natural person. Provided that an item of information collected by a company relates to a natural person, who can be identified, directly or indirectly, this information is personal data (CJEU, 2003: p. 27; A29DPWP, 2007, 2008). In other words, the criterion that has to be met, and which "makes" the data personal is not actual identification, but the capacity to identify, directly or indirectly, one person (Tene, 2008: p. 16). To sum up, if there is a capacity to identify the individual, to whom the "recorded heart rate" mentioned above relates, the data are personal and in particular health data (Panagopoulou-Koutnatzi, 2015b) and are fully regulated by the GDPR.

After having collected masses, sometimes, of personal data, which users produce "just by existing" (Powles & Hodson, 2017; Gray, 2015, Brabazon & Redhead, 2014), many firms behave as "owners" (Prins, 2006: pp. 223-224; Almunia, 2012) of this information (Cohen, 2000: p. 1375), by exchanging it (O'Neil, 2016: 151; Prins, 2006: p. 228; Hoofnagle, 2003; Michaels, 2008) or by further processing it (Crawford & Schultz, 2014). In this case, some scholars even talk about theft of humanistic property (Mann, 2000), this theft having been perpetrated by private enterprises, while others argue that natural persons should receive fair compensation for the collection, processing, exchange and use of their personal data (Litman, 2000), since there should be no free lunch when it comes to invading privacy (Laudon, 1996: p. 103).

Given the above practices, which show at least an important loss of the user's control over her personal data, this paper examines the validity and lawfulness of the data subject's consent to the processing of their personal data, studies the inability to anonymize such data and also, provides an overview of specific "private networks of knowledge", which any digital company is able to build (own and control) in violation of the fundamental right to non-discrimination.

2. The Subject's Consent to Data Processing

One of the fundamental principles of data protection law in Europe and beyond is respect for personal autonomy (Bottis, 2014: p. 148). Legal provisions on personal data safeguard constitutionally-protected rights to informational self-determination (Kang, Shilton, Estrin, Burke, & Hansen, 2012: p. 820). Hence, it has been consistently supported by authors that the fundamental (Article 8(1-2) of CFREU; Article 16(1) of TFEU) right to the protection of personal data refers to control by the subject over the processing of her data (Oostveen & Irion, 2016; Rengel, 2014). The key tool for a legal control of personal data is the subject's consent to the processing (Tene & Polonetsky, 2013: pp. 260-263; Solove, 2013: p. 1894; A29DPWP, 2011).

The European lawmaker recently regulated the protection of natural persons with regard to the processing of personal data and the free movement of such data (GDPR), and in this Regulation, took into account these aspects of control (Recitals (7) and (68) of GDPR) and legislated that the previous subject's consent shall be a necessary prerequisite for the lawfulness of data processing (Article 6(1)(a) of the GDPR). In particular, under the GDPR, the collection and processing (Article 4(2) of the GDPR) of personal data shall be lawful if the data subject has given consent to the processing of his or her personal data (Recital (4) and (42) of the GDPR) for one or more specific purposes (Article 6(1)(a), Recital (32) of the GDPR). Moreover, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Recitals (42), (43), Articles 7(4), 4(11) of the GDPR).

One would assume, therefore, that a "single mouse-click" on any privacy policy's box, by which users may give their consent, should not be considered to fulfill the criterion of "freely given, specific, informed and unambiguous" indication of the data subject's wishes by which the individual has to signify agreement to the processing. Quite the opposite is true: under Recital 32 of the GDPR, consent can also be given by "ticking a box, when visiting an internet website" (the repealed Directive 95/46/EC makes no mention of the capacity to give consent simply by ticking a box).

Thus, the data subject's consent to the collection and processing of her personal data may be validly and lawfully given by a single "mouse-click" on the box of a webpage, the terms of use and the privacy policy of which—almost—nobody reads (Turow, Hoofnagle, Mulligan, Good, & Grossklags, 2006: p. 724; Pingo & Narayan, 2016: p. 4; Gindin, 2009; Chesterman, 2017). Given that, as documented, in most cases the users "generously click" on any box that may "pop-up" (Vranaki, 2016: p. 29), private enterprises legally (and with individual's "freely given, specific, informed and unambiguous" wishes) process (e.g. collect, record, organize, structure, store, adapt, alter, retrieve, consult, use, disclose, disseminate, make available, combine, restrict, erase or destroy) personal data.

3. Anonymizing Data: A Failure?

In several cases, after having collected personal data, firms anonymize them. This means that "effective" measures are taken and data are further processed in a manner which renders the re-identification of the individual impossible (Hon, Millard, & Walden, 2011; Stalla-Bourdillon & Knight, 2017). Anonymization constitutes further processing (A29DPWP, 2014) and always comes after the collection of data. Hence, given the legislated validity of consent that users have already given often by a single "mouse-click", companies may legally anonymize their collection of personal data. Anonymized (ex-personal) data can be freely used e.g. shared with third parties, sold etc as the rules of data protection do not apply to "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (Recital (26) of the GDPR).

But in the age of Big Data, there is probably no safe way to render personal data truly anonymous (Scholz, 2017: p. 35; Schneier, 2015: pp. 50-53). Even after "anonymization", the data subject remains technologically identifiable (Ohm, 2010: p. 1701; Sweeney, 2000; Golle, 2006; Gymrek, McGuire, Golan, Halperin, & Erlich, 2013; Bohannon, 2013; Narayanan & Shmatikov, 2008). The inability to anonymize personal data in a Big Data environment is due to the collection and correlation of a huge volume of data from multiple sources. The result is the possibility to draw "countless conclusions" about an individual, who may be identified, directly or indirectly (Tene & Polonetsky, 2013: p. 257; Cunha, 2012: p. 270). In other words, anonymization can only be achieved in "Small Data" environments, given that the volume and the variety of data processed in the world of Big Data, facilitate and encourage (re)identification of any individual (Mayer-Schönberger & Cukier, 2013: p. 154).

We see, therefore, the anonymization of personal data, in a Big Data environment, portrayed as a failure. The same technology, which reassured us that we could not be identified, and so our personal data could be used for some noble purposes as, for example, medical research, now betrays us. A huge data set is almost magically, and reassuringly, turned anonymous, and then, adding a piece of information or two, it is turned back, some point later in time, to full identification (De Hert & Papaconstantinou, 2016: p. 184). If this is the case, where is our consent in this situation? A "single click" consent to this processing is from the outset pointless. The very specific purpose of the processing for which the individual has to give her initial consent has often, at the time of "mouse-click", not even been decided yet by the firm who is the controller (Mayer-Schönberger & Cukier, 2013: pp. 152-153; Giannakaki, 2014: pp. 263-264).

Thus, when users in fact ignore the final purpose (Steppe, 2017: p. 777; A29DPWP, 2008) for which consent is given (Bitton, 2014: p. 13), it is fair to support that they have lost control over their data (Solove, 2013: p. 1902). If no genuine consent can be given and if anonymization is indeed practically impossible, then there is no control at all (Carolan, 2016; Danagher, 2012). But this loss of control contrasts strongly with the goals and principles of the constitutional, in Europe, right to the protection of personal data. It defeats the *raison d' être* of all previous European legislation on data protection all the way since 1995.

4. Knowledge and the Fundamental Right to Non-Discrimination

Although the right to the protection of personal data is fundamental, probably not many people are aware of this right and much fewer have been documented to exercise powers which this right gives them (O'Brien, 2012; Hill, 2012). That people fail to exercise their rights or do not care about their personal data does not mean that this "apathy" should be "applauded" (Tene & Polonetsky, 2013: p. 263). A very important reason why it should be required that individuals demonstrate greater interest in their data protection, is that control over the processing of personal data enables the data controller to know (Mayer-Schönberger & Cukier, 2013: pp. 50-61; Cohen, 2000: p. 402).

In fact, in the Big Data environment control over the processing of personal data enables any firm to build its own "private networks of knowledge" (Powles & Hodson, 2017). These networks can lead, or perhaps has already led, to the accumulation of power, a power to an unprecedented extent and nature, resting in "private hands". This power may undermine the fundamental right to equality and non-discrimination (Article 21 of CFREU). As early as in 1993, Gandy spoke of a digital environment, where databases profiled consumers and sorted them into groups, each of which was given different opportunities (Gandy, 1993). Some years later, other scholars (Gilliom, 2001; Haggerty & Ericson, 2006) built on Gandy's theory and explained the manners in which new, at the time, tools and datasets were used by governments and private companies alike, so as to sort people and discriminate against them. Today, as these authors argue, private enterprises focus on human beings and study users' behaviors or movements or desires, so as to "mathematically" predict people's trustworthiness and calculate each person's potential as a worker, a criminal or a consumer. "Private algorithms", which process users' data, are seen as "weapons of math destruction" that threaten democracy and the universal value of equality (O'Neil, 2016: pp. 2-3, p. 151).

Today's "free" Internet is paid for mainly by advertising, for the needs of which tons of personal data are collected (Richards & King, 2016: pp. 10-13). Processing of these data with the help of cookies enables firms to identify the user and detect her online or even offline activities (Lam & Larose, 2017; Snyder, 2011). Thereafter, the user's data are used by private parties, to profile (Article 4(4) of the GDPR) people, to create "target groups", to which personalized ads may target the correct consumers (Förster & Weish, 2017: p. 19). In the Big Data environment, profiling or sorting consumers into groups may indeed be extremely effective. But the line between a legal sorting and profiling in favor of private interests and an unlawful, as contrary to the principle of equal treatment, discrimination based on personal data collected is blurry (Gandy, 2010; Article 21(1) of CFREU). It is also alarmingly disappearing, as users are being discriminated against on grounds of their personal data, not only during advertising, but in general, while private companies provide any services or just operate, by analyzing the users' data and "training their machines" (Mantelero, 2016: pp. 239-240; Crawford & Schultz, 2014: pp. 94-95, p. 98; Veale & Binns, 2017; Hastie, Tibshirani, & Friedman, 2009).

Given the correlations that Big Data allows and encourages, any private company that knows, for example, a user's gender, or her origin or her native language, may discriminate against her (Boyd & Crawford, 2011; Panagopoulou-Koutnatzi, 2017). This can happen by sorting or profiling, not only on the grounds of this information, but also on the grounds of other multiple personal data (Tene & Polonetsky, 2013: p. 240), which the private party may find by combining a huge volume of data, such as the exact address, where the user lives, or even the information that a consumer suffers from diabetes or that she is the mother of three minors (O'Neil, 2016: pp. 3-5, pp. 130-134, p. 151; Rubinstein, 2013: p. 76). Hence, a private company can use these data to create a system that will sort people into lists, put the most promising candidates on top, and "pick" the latter to fill the vacant posts in the company (O'Neil, 2016: pp. 3-5, pp. 130-134).

To sum up, sorting or profiling by "private algorithms", in favor of private interests and at the expense of people's fundamental right to equality and non-discrimination, analyzing and correlating data so as to project the "perfect ad" (See A29DPWP, 2013: p. 46) or promote the "appropriate good" at the "appropriate price" (Turow & McGuigan, 2014; EDPS, 2015: p. 19) or predict criminal behaviors (Chander, 2017: p. 1026) or "evaluate" the accused before sentencing courts (State v. Loomis, 2016), all these actions place almost insurmountable barriers in regulating the processing of personal data (Crawford & Schultz, 2014: p. 106). Knowledge and power seem to be accumulated in the hands of private entities in violation of people's fundamental rights. Firms may or do dictate "privacy policies and terms of processing of data", in conjunction with the continuous ticking of boxes with users' eyes closed (Manovich, 2011). This reality calls for solutions that will enable people to regain control over their personal data-over themselves (Mitrou, 2009).

5. Conclusion

By processing personal data, several economically and socially useful purposes have been achieved (Manovich, 2011; Prins, 2006: pp. 226-230; Knoppers & Thorogood, 2017). The processing of Big Data is even more promising. At the same time, however, the lawfulness of mass-processing of personal data in the Big Data environment is being questioned by many scholars. Although it is very important to examine this lawfulness in each emerging program or software, during the use of which consent is "grabbed by a mouse-click", it is much more important to understand the real conditions of this personal data processing, which many of us experience every day—or almost all of us experience many times each and every day.

The mass collection of personal data in an environment in which people do not meaningfully participate, in a setting of possibly opaque and discriminatory procedures (to predict, for example, people's behavior in general via the use of an algorithm, and then apply this prediction to a particular person), should concern all of us deeply. This is especially so, when people cannot know the purpose or even, ignore the very fact of processing and, hence, never give their consent in any meaningful way. The "consent fallacy" (i.e. the inability of the individual-websurfer to form and express free, conscious and informed choices, Mitrou, 2009: p. 466; Mitrou, 2017: p. 77) is accentuated at the highest possible degree. The processing of massive amounts of personal data, in combination with the accumulation of knowledge and power in "private networks" in violation of fundamental right to non-discrimination calls for a new progressive approach to legal provisions that protect personal data, and also, for the development of new technology inserting privacy protection in the very design of information systems dealing with Big Data (De Hert & Papaconstantinou, 2016).

The European legislator with the General Data Protection Regulation made a significant effort to protect people's rights on their personal data. Simultaneously, firms constantly devise and/or use new technologies of data-processing. This brings back to the discussion table some older academic opinions (Samuelson, 2000) that view commodification of personal data as a potential way, or even the only way, to regain control (Malgieri, 2016). Such an approach, hotly debated, falls outside the purposes of this paper but will be discussed in our future work.

References

A29DPWP (2007). *Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data*. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

A29DPWP (2008). *Article 29 Data Protection Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines*. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

A29DPWP (2011). *Article 29 Data Protection Working Party, Opinion 15/2011 on the Definition of Consent*. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

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

A29DPWP (2014). *Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques*. 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

Araka, I., Koutras, N., & Makridou, E. (2014). Access to Information: Evolution and digital divide. In M. Bottis (Ed.), *The History of Information, from Papyrus to the Electronic Document* (pp. 397-416). Athens: Nomiki Vivliothiki.

Battelle, J. (2005). *The Search: How Google and its Rivals Rewrote the Rules of Business and Transformed our Culture*. Boston, MA: Penguin Group.

Bitton, R. (2014). Intelligence Agents, Autonomous Slaves and the U.S. Supreme Court's Wrong (and Right) Concept of Personal Autonomy. *European Journal of Legal Studies, 7,* 1. https://doi.org/10.2139/ssrn.2402030

Bohannon, J. (2013). Genealogy Databases Enable Naming of Anonymous DNA Donors. *Science NY, 339,* 262. http://www.johnbohannon.org/NewFiles/DNA_privacy.pdf https://doi.org/10.1126/science.339.6117.262

Bottis, M. (2014). Law and Information: A "Love-Hate" Relationship. In M. Bottis (Ed.), *The History of Information, from Papyrus to the Electronic Document* (pp. 141-152). Athens: Nomiki Vivliothiki.

Boyd, D., & Crawford, K. (2011). Six Provocations for Big Data. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.* https://ssrn.com/abstract=1926431 https://doi.org/10.2139/ssrn.1926431

Brabazon, T., & Redhead, S. (2014). *Theoretical Times: Reproletarianization*. Libsyn. https://archive.org/details/TheoreticalTimesReproletarianization

Brabazon, T. (2015). Digital Fitness: Self-Monitored Fitness and The Commodification of Movement, *Communication Politics & Culture, 48,* 1-23.

Carolan, E. (2016). The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles. *Computer Law and Security Review, 32,* 462-273. https://doi.org/10.1016/j.clsr.2016.02.004

CFREU (2000). Charter of Fundamental Rights of the European Union. *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/

Chesterman, S. (2017). Privacy and Our Digital Selves. *The Straits Times*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3033449

CJEU (2003). *Court of Justice of the European Union. Judgment of 6.11.2003*. Case C-101/01, Criminal proceedings against Bodil Lindqvist. Reference for a preliminary ruling: Göta hovrätt, Sweden. EU:C:2003:596. http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=510324

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

Committee on Commerce, Science, and Transportation (2013). *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Staff Report for Chairman Rockefeller.* USA: United States Senate. http://educationnewyork.com/files/rockefeller_databroker.pdf

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

Cunha, M. V. (2012). Review of the Data Protection Directive: Is There Need (and Room) for a New Concept of Personal Data? In S. Gutwirth et al. (Eds.), *European Data Protection: In Good Health?* (pp. 267-284). New York: Springer. https://doi.org/10.1007/978-94-007-2903-2_13

Danagher, L. (2012). An Assessment of the Draft Data Protection Regulation: Does It Effectively Protect Data? *European Journal of Law and Technology, 3.* http://ejlt.org/article/view/171/260

De Hert, P., & Papaconstantinou, V. (2016). The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? *Computer Law and Security Review, 32,* 179-194. https://www.sciencedirect.com/science/article/pii/S0267364916300346 https://doi.org/10.1016/j.clsr.2016.02.006

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.*

European Commission (2017). *Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service.* European Commission, Press Release. http://europa.eu/rapid/press-release_IP-17-1784_en.htm

Förster, K., & Weish, U. (2017). Advertising Critique: Themes, Actors and Challenges in a Digital Age. In G. Siegert, M. B. Rimscha, & S. Grubenmann (Eds.), *Commercial Communication in the Digital Age, Information or Disinformation?* (pp. 15-35). Berlin/Boston: Walter de Gruyter GmbH. https://doi.org/10.1515/9783110416794-002

Gandy, O. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Michigan: Westview Press.

Gandy, O. (2010). Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems. *Ethics and Information Technology, 12*, 29-42. https://link.springer.com/article/10.1007/s10676-009-9198-6 https://doi.org/10.1007/s10676-009-9198-6

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, Repealing the Directive 95/46/EC.*

Giannakaki, M. (2014). The Value of Information in the Age of "Big Data": From Web 1.0 to Web 3.0. In M. Bottis (Ed.), *The History of Information, from Papyrus to the Electronic Document* (pp. 259-272). Greece: Nomiki Vivliothiki.

Gilliom, J. (2001). *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy.* Chicago, IL: Series in Law and Society, University of Chicago Press.

Gindin, S. E. (2009). Nobody Reads Your Privacy Policy or Online Contract: Lessons Learned and Questions Raised by the FTC's Action against Sears. *Northwestern Journal of Technology and Intellectual Property, 8,* 1-37. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1094&context=njtip

Golle, P. (2006). Revisiting the Uniqueness of Simple Demographics in the US Population. In *Proceedings of the 5th ACM Workshop on Privacy in the Electronic Society (WPES'06)* (pp. 77-80). New York: ACM. https://dl.acm.org/citation.cfm?id=1179615

Gray, J. (2015). *The Soul of a Marionette: A Short Enquiry into Human Freedom*. UK: Allen Lane.

Gymrek, M., McGuire, A., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying Personal Genomes by Surname Inference. *Science, 339,* 321-324. https://www.ncbi.nlm.nih.gov/pubmed/23329047

Haggerty, K., & Ericson, R. V. (2006). *The New Politics of Surveillance and Visibility.* Toronto: University of Toronto Press, Scholarly Publishing Division.

Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction* (2nd ed.). Stanford, CA: Stanford University. https://web.stanford.edu/~hastie/Papers/ESLII.pdf https://doi.org/10.1007/978-0-387-84858-7

Hill, K. (2012). *Max Schrems, The Austrian Thorn in Facebook's Side*. 7 February 2012. Forbes. https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/

Himma, E. K. (2007). A Preliminary Step in Understanding the Nature of a Harmful Information-Related Condition: An Analysis of the Concept of Information Overload. *Ethics and Information Technology, 9,* 259-272. https://doi.org/10.1007/s10676-007-9140-8

Hon, W. K., Millard, C., & Walden, I. (2011). The Problem of "Personal Data" in Cloud Computing—What Information Is Regulated? The Cloud of Unknowing. *International Data Privacy Law, 1,* 211-228. https://doi.org/10.1093/idpl/ipr018

Hoofnagle, C. J. (2003). Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement. *Berkeley Law Scholarship Repository, 29,* 595-638.

https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1677&context=facpubs

Hugenholtz, B., & Guibault, L. (2006). The Future of the Public Domain: An Introduction. In L. Guibault, & B. Hugenholtz (Eds.), *The Future of the Public Domain, Identifying the Commons in Information Law* (pp. 1-6). The Netherlands: Kluwer Law International.

Kang, J., Shilton, K., Estrin, D., Burke, J., & Hansen, M. (2012). Self-Surveillance Privacy. *Iowa Law Review, 97,* 809-847. http://heinonline.org/HOL/Page?handle=hein.journals/ilr97&div=24&g_sent=1&casa_token=&collection=journals#

King, N., & Forder, J. (2016). Data Analytics and Consumer Profiling: Finding Appropriate Privacy Principles for Discovered Data. *Computer Law & Security Review, 32,* 696-714. https://doi.org/10.1016/j.clsr.2016.05.002

Knoppers, B. M., & Thorogood, A. M. (2017). Ethics and Big Data in Health, Big Data Acquisition and Analysis. *Current Opinion in Systems Biology, 4,* 53-57.

Koelman, J. K. (2006). The Public Domain Commodified: Technological Measures and Productive Information Use. In L. Guibault, & B. Hugenholtz (Eds.), *The Future of the Public Domain, Identifying the Commons in Information Law* (pp. 105-119). The Netherlands: Kluwer Law International.

Lam, B. H., & Larose, J. C. (2017). *United States: FTC Asked to Investigate Google's Matching of Bricks to Clicks*. 25 September 2017, Mondaq. http://www.mondaq.com/article.asp?articleid=630914&email_access=on&chk=2167746&q=1536832

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

Lessig, L. (2006). *Code and Other Laws of Cyberspace, Version 2.0*. New York: Basic Books.

Lidstone, H. (2014). *Using the Cloud: Trade Secrets and Confidential Information Aren't So Secret* (pp. 1-11). USA: Burns, Figa & Will, P.C. https://doi.org/10.2139/ssrn.2358472

Litman, J. (2000). Information Privacy/Information Property. *Stanford Law Review, 52,* 1283-1313. https://ssrn.com/abstract=218274 https://doi.org/10.2139/ssrn.218274

Malgieri, G. (2016). "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution? *Journal of Internet Law, 20*, 1-17. https://ssrn.com/abstract=2916079

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

Manovich, L. (2011). Trending: The Promises and the Challenges of Big Social Data. In M. K. Gold (Ed.), *Debates in the Digital Humanities*. Minneapolis, MN: The University of Minnesota Press. http://manovich.net/index.php/projects/trending-the-promises-and-the-challenges-of-big-social-data

Mantelero, A. (2016). Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. *Computer Law & Security Review, 32,* 238-255. https://doi.org/10.1016/j.clsr.2016.01.014

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. UK: John Murray.

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

Mitrou, L. (2009). The Commodification of the Individual in the Internet Era: Informational Self-Determination or "Self-Alienation"? In M. Bottis (Ed.), *Proceedings of the 8th International Conference of Computer Ethics Philosophical Enquiry (CEPE 2009)* (pp. 466-484). Greece: Nomiki Vivliothiki.

Mitrou, L. (2017). *The General Data Protection Regulation, New Law, New Obligations, New Rights*. Greece: Sakkoulas.

Morozov, E. (2011). *The Net Delusion, the Dark Side of Internet Freedom*. USA: Public Affairs.

Narayanan, A., & Shmatikov, V. (2008). Robust De-Anonymization of Large Sparse Datasets. In *IEEE Symposium on Security and Privacy* (pp. 111-125). Oakland, CA: IEEE. http://ieeexplore.ieee.org/document/4531148/

O'Brien, K. (2012). Austrian Law Student Faces down Facebook. *The New York Times*, 5 February 2012. https://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html

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

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review, 57,* 1701-1777. https://www.uclalawreview.org/pdf/57-6-3.pdf

Oostveen, M., & Irion, K. (2016). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? In Bakhoum, G., & Mackenordt, S. (Eds.), *Personal Data in Competition, Consumer Protection and IP Law—Towards a Holistic Approach?* Berlin: Springer. https://ssrn.com/abstract=2885701

Panagopoulou-Koutnatzi, F. (2015a). THE internet of Things (IoT): The Colonization of Everyday Life or a New Technological Challenge? In M. Bottis, E. Alexandropoulou, & I. Igglezakis (Eds.), *Proceedings from 6th ICIL 2014: Lifting the Barriers to Empower the Future of Information Law and Ethics* (pp. 243-262). Greece: University of Macedonia.

Panagopoulou-Koutnatzi, F. (2015b). Disclosure of Personal Medical Data with the Permission of the Hellenic Data Protection Authority (HDPA): Institutional Valuation. *Administrative Law Journal, 6,* 755-771.

Panagopoulou-Koutnatzi, F. (2017). New Rights under the Data Protection Regulation: A Constitutional Appraisal. *Administrative Law Journal, 1,* 81-98.

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

Petrovic, O. (2017). The Internet of Things as Disruptive Innovation for the Advertising Ecosystem. In G. Siegert, M. B. Rimscha, & S. Grubenmann (Eds.), *Commercial Communication in the Digital Age, Information or Disinformation?* (pp. 183-205). Germany: Walter de Gruyter GmbH. https://doi.org/10.1515/9783110416794-011

Picker, C. R. (2008). Competition and Privacy in Web 2.0 and the Cloud. *Northwestern University Law Review Colloquy, 103,* 1-12.

https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1124&context=nulr_online
https://doi.org/10.2139/ssrn.1151985

Pingo Z., & Narayan, B. (2016). When Personal Data Becomes Open Data: An Exploration of Lifelogging, User Privacy, and Implications for Privacy Literacy. In A. Morishima, A. Rauber, & C. L. Liew (Eds.), *Digital Libraries: Knowledge, Information and Data in an Open Access Society—18th International Conference on Asia-Pacific Digital Libraries, Tsukuba, Japan* (pp. 3-9). Japan: Springer International.

Powles, J., & Hodson, H. (2017). Google DeepMind and Healthcare in an Age of Algorithms. *Health and Technology, 7,* 351-367. https://doi.org/10.1007/s12553-017-0179-1

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). The Netherlands: Kluwer Law International.

Rengel, A. (2014). Privacy as an International Human Right and the Right to Obscurity in Cyberspace. *Groningen Journal of International Law, 2,* 33-54.
https://grojil.files.wordpress.com/2015/04/grojil_vol2-issue2_rengel.pdf

Richards, N. M., & King, J. (2016). Big Data and the Future for Privacy. In F. X. Olleros, & M. Zhegu (Eds.), *Handbook of Research on Digital Transformations* (pp. 272-290). Cheltenham: Elgar. https://ssrn.com/abstract=2512069
https://doi.org/10.4337/9781784717766.00021

Rubinstein, I. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law, 3,* 74-87. https://doi.org/10.1093/idpl/ips036

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

Schneier, B. (2015). *Data and Goliath, The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company.

Scholz, M. T. (2017). *Big Data in Organizations and the Role of Human Resource Management, a Complex Systems Theory-Based Conceptualization*. New York: Peter Lang.

Snyder, W. (2011). Making the Case for Enhanced Advertising Ethics: How a New Way of Thinking about Advertising Ethics May Build Consumer Trust. *Journal of Advertising Research, 51,* 477-483.
http://www.journalofadvertisingresearch.com/content/51/3/477
https://doi.org/10.2501/JAR-51-3-477-483

Solove, D. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review, 126,* 1880-1903.
https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/

Stalla-Bourdillon, S., & Knight, A. (2017). Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization, and Personal Data. *Wisconsin International Law Journal, 34,* 284-322. https://eprints.soton.ac.uk/400388/

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

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

Summers, L., & DeLong, J. B. (2001). The "New Economy": Background, Historical Perspective, Questions and Speculations. *Economic Review, Federal Reserve Bank of Kansas City, 86,* 29-59.

Sweeney, L. (2000). *Simple Demographics Often Identify People Uniquely.* Data Privacy Working Paper No. 3, Pittsburgh, PA: Carnegie Mellon University. https://dataprivacylab.org/projects/identifiability/paper1.pdf

Tene, O. (2008). What Google Knows: Privacy and Internet Search Engines. *Utah Law Review, 4,* 1433-1492.

Tene, O. (2011). Privacy: The New Generations. *International Data Privacy Law, 1,* 15-27. https://doi.org/10.1093/idpl/ipq003

Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property, 11,* 239-273. https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

TFEU (2012). Treaty on the Functioning of the European Union. *Official Journal C 326,* 26/10/2012 P. 0001-0390. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT

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). https://na-production.s3.amazonaws.com/documents/data-and-discrimination.pdf

Turow, J., Hoofnagle, C. J., Mulligan, D. K., Good, N., & Grossklags, J. (2006). The FTC and Consumer Privacy in the Coming Decade. *I/S: A Journal of Law and Policy for the Information Society, 3,* 723-749. https://repository.upenn.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1066&context=asc_papers

Veale, M., & Binns, R. (2017). Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data. *Big Data & Society, 4,* 2. https://ssrn.com/abstract=3060763

Vranaki, A. (2016). *Social Networking Site Regulation: Facebook, Online Behavioral Advertising, Power and Data Protection Laws.* Queen Mary School of Law Legal Studies Research Paper No. 221, 2-34. https://ssrn.com/abstract=2731159