Review of European Studies; Vol. 10, No. 4; 2018
ISSN 1918-7173 E-ISSN 1918-7181
Published by Canadian Center of Science and Education

Privacy and Web 3.0: Implementing Trust and Learning From Social Networks

George Bouchagiar[1]

[1] Institute for Information Law (IViR), Amsterdam, The Netherlands

Correspondence: George Bouchagiar, Institute for Information Law (IViR), Amsterdam, The Netherlands.

Received: September 11, 2018 Accepted: October 8, 2018 Online Published: August 27, 2018

doi:10.5539/res.v10n4p16 URL: https://doi.org/10.5539/res.v10n4p16

Abstract

After having shifted from Web 1.0 to Web 2.0, scientists welcome the advent of Web 3.0, an environment where meaning is added to data. While in the Semantic Web people are no longer users, but part of the emerging applications, producers, subjects and beneficiaries of the Big Data, however, opaque processing of personal data poses tremendous risks and dangers for individuals. Given the new era of Big Data this paper studies firms' purposes and practices to detect some emerging privacy risks. Moreover, theories that deal with social networks are examined to conclude that, even if people state that they value their privacy, however, they often disclose a huge volume of personal information. Taking into account that today's European concept of privacy is conceptualized in negative terms this paper also proposes the implementation of trust and loyalty into the privacy concept through flexible fiduciary laws. Furthermore, data portability is discussed to detect its potential as a strategic feature, a key tool that will enhance trust. Finally, further scenarios and proposals are submitted, in our attempt to answer the question whether the European concept of privacy could be re-shaped for the benefit of individuals.

Keywords: personal data, Web 3.0, privacy, fiduciary laws, data portability

1. Introduction

In 1983, Time magazine nominated the Personal Computer as "the machine of the year" to announce the entry of the Informational Age into our homes[1]. In 2006, a computer was again displayed in the above magazine's cover, albeit, this time the computer screen was a mirror reflecting the person of the year: "*You.*", the very user, the hero of the Information Age[2].

After having shifted from Web 1.0 (First Era)[3] to Web 2.0 (Second Era)[4], scientists speak of the Semantic Web[5] (Web 3.0)

[1]See Time, The Computer, Machine of the Year | Jan. 3, 1983: http://content.time.com/time/covers/0,16641,19830103,00.html.

[2]See Time, December 25, 2006 | Vol. 168 No. 26. http://content.time.com/time/magazine/0,9263,7601061225,00.html. See also Mirko Tobias Schäfer, Bastard Culture! How user participation transforms cultural production, 2011, Amsterdam University Press, pp. 1-256, at p. 9.

[3] The First Era (Web 1.0) corresponds to the early years of the World Wide Web. The web was a collection of mainly static pages that held information and content created by firms or organizations, which had created the relevant site or web page. The creation of content was performed by experts and it was not so easy to acquire personal web pages. Thus, users were mere information consumers. See Juan M. Silva, Abu Saleh Md. Mahfujur Rahman, Abdulmotaleb El Saddik, Web 3.0: A Vision for Bridging the Gap between Real and Virtual, in Proceedings of the 1st ACM international workshop on Communicability design and evaluation in cultural and ecological multimedia system, Vancouver, British Columbia, Canada, October 31, 2008, pp. 9-14, at p. 10. Available at http://delivery.acm.org/10.1145/1470000/1462042/p9-silva.pdf?ip=146.50.68.122&id=1462042&acc=ACTIVE%20SERVICE&key=0C390721DC3021FF%2E86041C471C98F6DA%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1522471038_1b13b576240ef9abe4e5a87afad829ae.

[4] Web 2.0, the second generation of the Web, is defined by the empowerment of the end user to actively create content and participate in the Web to expose herself and relate to others. Attention is drawn to technologies that enable collaboration, such as social networks. Relevant tools are easy to use and this allows almost anyone to publish many different multimedia contents. See Juan M. Silva, Abu Saleh Md. Mahfujur Rahman, Abdulmotaleb El Saddik, Web 3.0:

that tries to extend models using a series of standard languages that enable the description of Web resources to be enriched –and to become semantically accessible. To do so, Web 3.0 is based on two concepts: semantic tagging of resources, so that information can be understood by humans and computers, and the development of intelligent agents[6] that are capable of operating with those resources and inferring new knowledge from them[7]. To put it simply, the Semantic Web[8] adds meaning to web documents from the sense of content and metadata[9].

And how much information is on the Web? There is too much.

People disclose a huge volume of data on a daily basis, in innumerous websites and during countless online activities, such as –to name but a few– while communicating via e-mails, interacting in social networks, or exercising their jobs. Focusing on social networks[10], millions of users reveal a lot about the most intimate details of their lives, which may cover all aspects of the individual's life[11]. Thus, present-day abundance of social network profiles raises further issues with regard to privacy[12].

A Vision for Bridging the Gap between Real and Virtual, id, at p. 10. See also Federica Cena, Rosta Farzan Pasquale Lops, Web 3.0: Merging Semantic Web with Social Web, HT '09 Proceedings of the 20th ACM conference on Hypertext and hypermedia, pp. 385-386, Torino, Italy, June 29 - July 01, 2009, ACM, New York. Available at https://dl.acm.org/citation.cfm?doid=1557914.1558002.

[5] See Tim Berners-Lee, James Hendler, Ora Lassila, The Semantic Web, Scientific American, Vol. 284, No. 5 (May 2001), pp. 34-43. Available at http://www.jstor.org/stable/26059207?seq=1#page_scan_tab_contents.

[6] J. Hendler, Agents and the semantic web, IEEE Intelligent Systems, Volume 16, Issue 2, Mar-Apr 2001, pp. 30–37. Available at http://ieeexplore.ieee.org/abstract/document/920597/?reload=true.

[7] J. M. Morales-del-Castillo, Eduardo Peis, Antonio A. Ruiz, E. Herrera-Viedma, Recommending biomedical resources: A fuzzy linguistic approach based on semantic web, International Journal of Intelligent Systems, Volume25, Issue12, Special Issue: New Trends for Ontology-Based Knowledge Discovery, December 2010, pp. 1143-1157. Available at https://onlinelibrary.wiley.com/doi/full/10.1002/int.20447.

[8] See also Maria Giannakaki, The value of information in the age of 'Big Data': from Web 1.0 to Web 3.0, in Maria Bottis, The history of Information: From papyrus to the electronic document, Nomiki Bibliothiki S.A., 2014, pp. 259-272, at p. 259, mentioning that that in the age of the semantic web importance is attached to raw data, which is collected from different sources to discover, assemble and correlate a huge volume of information.

[9] Bujar Raufi, Florije Ismaili, Jaumin Ajdari, Xhemal Zenuni, Knowledgebase Harvesting for User-Adaptive Systems Through Focused Crawling and Semantic Web, in Proceedings of the 17th International Conference on Computer Systems and Technologies 2016, Palermo, Italy (June 23 - 24, 2016), pp. 323-330, at p. 324 (where it is also mentioned that "[…] *semantic web tends to add semantic meaning or metadata to every document on the web so they can be machine processable as well as easily retrievable. The Semantic Web brings structure to the meaningful content of Web pages, creating an environment where different software agents such as crawlers can move around from page to page and can readily carry out sophisticated tasks for users. The process of publishing a meaningful content to the web requires a confluence between users as well as adjusting to frequent technology changes related to semantic web* […]").

[10] In the social context, a network consists of a set of individuals and of the links among them ("[…] *Links between pairs of individuals might represent a wide range of connections, including such activities as friendship, advice seeking, informational communication, and material transfers* […]"). See David Krackhardt & Robert N. Stern, Informal Networks and Organizational Crises: An Experimental Simulation, 51 Social Psych. Q. 123, 127 (1988). Social networking sites are a kind of an online service, which aims to create social relations between people, who share common interests and activities. Information sharing with one's public or private contacts is the primary function of the above networks. Krasnova H., Spiekermann S., Koroleva K., & Hildebrand T., Online social networks: why we disclose, Journal of Information Technology, 25(2), 2010 109-125, DOI:10.1057/JIT.2010.6. Available at SSRN: https://ssrn.com/abstract=2050898.

[11] J.C. Buitelaar, Post-mortem privacy and informational self-determination, Ethics and Information Technology, 2017, Vol. 19, Iss. 2, pp. 129-142, at pp. 129, 131. Available at https://link.springer.com/article/10.1007/s10676-017-9421-9.

[12] Regan argues that, today, the abundance of these profiles suggests that privacy should be framed more as a common good, while at the same time the normative underpinnings of the value of privacy are shared among members of society. See P.M. Regan, Privacy and the common good: Revisited, in B. Roessler & M. Mokrosinska (eds), Social dimensions of privacy: interdisciplinary perspectives, 2015, London: Cambridge University Press, pp. 50-70. Available at https://www.researchgate.net/publication/290315805_Privacy_and_the_common_good_Revisited. Of course, privacy is not the only issue that is raised: for the potential of social networks as platforms used by terrorists, see Marie-Helen

For instance, job seekers reveal online information that they would not disclose during an "offline interview", while minors may reveal sensitive data, like their sexual orientation or their ethnic origins, just by updating their status, or posting a comment, or uploading images[13]. In fact, people can disclose their deepest secrets and, thus, some authors argue that privacy needs to be reshaped. Is it about secrecy[14]? Is it a right to be let alone[15]?

Today's users can access social networks' platforms and disclose their personal data[16], such as their physical location (for instance, GPS or IP location), while they may not be aware that the very location –of their mobile device– is constantly being recorded, regardless of use –or non use– of the device[17]. Moreover, people's behaviors and relationships have changed as well. Our kids may have "more friends" than us –and we are not one of them– while, at the same time, a social network's platform may be regarded as a place where minors (and people in general) exchange information and communicate with their peers; enter a parent and the party is over[18]. There is no distinction between lovers, schoolmates, and strangers and they are all, thus, sorted into same group ("friends")[19].

Given the above radical changes, this paper studies the processing of personal data in the age and the economy of Big Data to detect purposes –and risks– of such practices. Furthermore, the hedonic use of social networks and several theories (such as the social capital theory, altruism and reciprocity), with regard to such networks, are examined to argue that,

---

Maras, Social Media Platforms: Targeting the "Found Space" of Terrorists, Journal of Internet Law, August 2017, pp. 3-9. Available at https://www.researchgate.net/publication/321549900_Social_Media_Platforms_Targeting_the_Found_Space_of_Terrorists. Social networks, however, can also be used to achieve several socially useful purposes. For instance, with regard to their significant role in disaster management, see Jooho Kim, Makarand Hastak, Social networks analysis: Characteristics of online social networks after a disaster, in International Journal of Information Management, February 2018, Vol. 38(1), pp. 86-96. Available at https://www.researchgate.net/publication/322175764_Social_network_analysis_Characteristics_of_online_social_networks_after_a_disaster. For their effects on academic achievement, see Robert M. Bond, Volha Chykina, Jason J. Jones, Social network effects on academic achievement, The Social Science Journal, Volume 54, Issue 4, December 2017, pp. 438-449, available at https://www.sciencedirect.com/science/article/pii/S0362331917300605.

[13] See, amongst others, A. Acquisti, C. Fong, An Experiment in Hiring Discrimination Via Online Social Networks, July 17, 2015. Available at SSRN: https://ssrn.com/abstract=2031979 or http://dx.doi.org/10.2139/ssrn.2031979/.

[14] For instance, Strahilevitz argues that privacy is not about secrecy. Indeed, a sexual intercourse needs more than one, people tell others about medical ailments to unburden, and sharing most intimate information with those, who are expected to keep it secret, promotes friendship and intimacy. See Strahilevitz Lior, A Social Networks Theory of Privacy, December 2004, U Chicago Law & Economics, Olin Working Paper No. 230; U of Chicago, Public Law Working Paper No. 79, at. p. 5. Available at SSRN: https://ssrn.com/abstract=629283 or http://dx.doi.org/10.2139/ssrn.629283. However, as others claim, there is a relation between privacy and secrecy ("[…] *right to secrecy* […] *to limiting the knowledge of others about oneself* […]"). See Cavoukian A. & Tapscott D., Who Knows: Safeguarding Your Privacy in a Networked World, McGraw-Hill, New York, 1997.

[15] The right to privacy is an old subject of legal discussion and has been known as the "right to be let alone". See S. Warren & L. Brandeis, The right to Privacy, Harvard Law Review vol. 4, ed. 5, 1890, pp. 193-220. For the function of privacy as a tool for limiting –the ability of third parties to– access individual's personal data, see Neil M. Richards & Jonathan H. King, Big Data and The Future for Privacy, Handbook of Research on Digital Transformations, Elgar, 2016, p. 8.

[16] "Personal data" means "[…] *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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* […]". See Article 4(1) of 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), hereinafter referred to as "GDPR".

[17] Omer Tene, Privacy: The new generations, International Data Privacy Law, Volume 1, Issue 1, 1 February 2011, pp. 15-27, https://doi.org/10.1093/idpl/ipq003. Available at https://academic.oup.com/idpl/article/1/1/15/759641.

[18] Omer Tene, Privacy: The new generations, id.

[19] See Danah Boyd, Friends, Friendsters, and MySpace Top 8: Writing Community Into Being on Social Network Sites, December 4, 2006, First Monday, Volume 11, Number 12, available at http://firstmonday.org/article/view/1418/1336.

although people may state that they value their privacy, albeit, they rarely refuse to share personal information. Current concept of privacy is brought to the discussion table to comment on its negative approach and to propose the introduction of trust and loyalty through flexible fiduciary laws. Moreover, data portability, one of the most important rights that the GDPR introduces, is studied to support its potential as a strategic element that will safeguard and enhance trust. Finally, further proposals are submitted to support that the European concept of privacy could, indeed, be re-shaped for the benefit of individuals.

2. Personal Data in the Age and the Economy of Big Data

Some authors referring to the wealth of data flooding the digital environment –often described as Big Data– have defined Web 3.0 as "*Semantic Web technologies integrated into, or powering, large-scale Web applications*"[20]. Web 3.0 could be understood as a phenomenon in which individuals are no longer users; they are part of the applications that emerge and disappear; they are also producers, subjects and beneficiaries of Big Data[21]. In particular, Big Data refers to the exponential growth and availability of data in an environment, where the three "V" characteristics are identified; the Volume of data, which is collected and processed, the Velocity, meaning the speed, with which data is being produced and processed, and the Variety of sources[22]. This environment provides further opportunities for understanding or predicting individuals' behavior and, thus, firms can expand their knowledge about a person without her knowledge or consent[23]. Indeed, people have little or no idea with regard to what or ways in which data is collected, processed, shared or exchanged[24] with third parties[25].

In 2018, life, including social connections or even love[26], happens online and, hence, it is difficult to name an aspect of

[20] See Jim Hendler, Web 3.0 emerging, Computer, 2009, Vol. 42, No. 1, pp. 111-113. Available at https://dl.acm.org/citation.cfm?id=1512177.

[21] See David Kreps, Kai Kimppa, Theorising Web 3.0: ICTs in a changing society, Information Technology & People, 2015, Vol. 28, Issue 4, pp. 726-741, at p. 734, https://doi.org/10.1108/ITP-09-2015-0223. Available at https://www.emeraldinsight.com/doi/pdfplus/10.1108/ITP-09-2015-0223.

[22] Nancy J. King & Jay Forder, Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data, Computer Law & Security Review 32, 2016, 696-714, p. 698. Some authors add more characteristics, such as the "Veracity", which refers to the way data should be used in order to create necessary trust and ensure reliability. See Maria Giannakaki, The value of information in the age of 'Big Data': from Web 1.0 to Web 3.0, id, at p. 262. Others identify two additional dimensions of Big Data; variability and complexity. The former is evidenced by the fact that data flows can be highly inconsistent with periodic peaks, while the latter is manifested in the nature of Big Data itself. It is not only structured but also unstructured and coming from multiple sources. See Richard Herschel, Virginia M. Miori, Ethics & Big Data, Technology in Society 49 (2017), pp. 31-36, at p. 31, mentioning that "[…] *Big Data is all about capturing, storing, sharing, evaluating, and acting upon information that humans and devices create and distribute using computer-based technologies and networks* […]" and pointing out that we are now generating 2.5 quintillion bytes of data, so much that 90% of the data in the world today has been created in the last couple of years. Available at https://www.researchgate.net/publication/314463176_Ethics_Big_Data.

[23] For some ethical issues with regard to privacy, confidentiality, transparency and identity, see Jonathan H. King & Neil M. Richards, What's Up With Big Data Ethics? 2014, Radar, O'Reilly Media, available at http://radar.oreilly.com/2014/03/whats-up-with-big-data-ethics.html.

[24] A secondary market has been created with regard to personal data: Data brokers may be defined as professionals who operate on a secondary market, such as businesses that facilitate the circulation and enrichment of data. See Commission Nationale De L' Informatique Et Des Libertés (CNIL), 36th Activity Report, 2015, To Protect Personal Data, Support Innovation, Preserve Individual Liberties, pp. 31-32 ("Data brokers: the oil and the iceberg"). Available at https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_2015_gb.pdf. As CNIL puts it, data brokerage aims to aggregate data, then redistribute it for a variety of purposes, which are focused –amongst others– on commercial targeting (for example, direct marketing, advertising, customer experience enhancement) or checking people's characteristics (namely trustworthiness, creditworthiness, identity etc).

[25] See Neil M. Richards, Jonathan H. King, Big Data Ethics, Wake Forest Law Review, Vol. 49, 2014, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2384174, pp. 393-432, at p. 393. See also Neil M. Richards, Jonathan H. King, Three Paradoxes of Big Data, 66 Stan. L. Rev. Online, pp. 41-46, September 3, 2013, available at https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_StanLRevOnline_41_RichardsKing.pdf.

[26] See Lainey Feingold, Digital Accessibility and The Quest For Online Equality, Journal of Internet Law, Oct. 2017, pp. 3-12, at p. 3.

present-day society in which online access does not play a part. Thereafter, during innumerous online activities, a huge volume of personal data is produced, collected[27] and processed[28].

Does an item of information, e.g. one's pattern of sleep, which may be provided while using a smart phone app, constitute personal data?

In the age of Big Data, processing of a huge volume of data[29] not only enables firms to draw innumerous conclusions that relate to one person but also encourages identification of an individual. So when the above pattern of sleep relates to an individual, who can be identified, it does constitute personal data[30]. This means that it is not the actual identification, but the capacity to identify one person[31] that makes the data personal.

So, why do firms process our personal data?

Today, what we deal with is the monster of a "free" Internet[32] paid for by advertising targeted on the basis of an unprecedented level of surveillance of human lives[33]. Data processing enables firms not only to identify an individual or detect her activities[34] but also to profile[35] natural persons and target groups, to which firms address personalized ads[36].

For example, Google used billions of credit-card transaction records to prove that its online ads are prompting people to make purchases even when they happen in brick-and-mortar stores[37]. In other words, Google's program (Store Sales

[27] See Commission Nationale De L' Informatique Et Des Libertés (CNIL), 36th Activity Report, 2015, id, at p. 35 ("From connected devices to autonomous devices: What freedoms subsist in a robotised world?"), mentioning that "[…] *constant data capture in our everyday environment is a real novelty* […]".

[28] Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property Volume 11, Issue 5, pp. 239-273, 2013.

[29] For instance, robots are becoming *cobots* (collaborative robots) that can act with humans. To do so, they collect far more data. This highlights a fundamental ethical paradox in the data protection domain: to be more autonomous, a machine must, in fact, become more dependent on personal data. See Commission Nationale De L' Informatique Et Des Libertés (CNIL), 36th Activity Report, 2015, id, at p. 36 ("From connected devices to autonomous devices: What freedoms subsist in a robotised world?").

[30] The meaning of personal data is unsuccessfully very wide. See Maria Bottis, Surveillance, data protection and libraries in Europe and the US-notes on an empirical data case study on surveillance and Greek academic libraries, in Maria Bottis (ed.), Privacy and Surveillance, Current Aspects and Future Perspectives, Nomiki Bibliothiki, 2012, pp. 272-282, at p. 273. Even IP or cookies may constitute personal data. See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Jun. 20, 2007; Opinion 1/2008 on data protection issues related to search engines, April 4, 2008.

[31] Omer Tene, What Google Knows: Privacy and Internet Search Engines, October 1, 2007, Utah Law Review, available at SSRN: https://ssrn.com/abstract=1021490 or http://dx.doi.org/10.2139/ssrn.1021490, at p. 16.

[32] Neil M. Richards & Jonathan H. King, Big Data and The Future For Privacy, Handbook of Research on Digital Transformations, Elgar, 2016, at p. 11. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2512069.

[33] Zuckerman E., The Internet's Original Sin, The Atlantic, 2014, Available at https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/#. As Zuckerman aptly puts it, "[…] *20 years in to the ad-supported web, we can see that our current model is bad, broken, and corrosive. It's time to start paying for privacy, to support services we love, and to abandon those that are free, but sell us—the users and our attention—as the product* […]".

[34] Wally Snyder, Making the Case for Enhanced Advertising Ethics: How a New Way of Thinking About Advertising Ethics May Build Consumer Trust, in Journal of Advertising Research, Vol. 51, issue 3, 2011, pp. 477-483. Available at http://www.journalofadvertisingresearch.com/content/51/3/477.full.pdf+html.

[35] Under Article 4(4) of GDPR "[…] *'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements* […]".

[36] See Kati Förster & Ulrike Weish, Advertising Critique: Themes, Actors and Challenges in a Digital Age, in Gabriele Siegert, M. Bjørn von Rimscha, Stephanie Grubenmann (eds), Commercial Communication in the Digital Age, Information or Disinformation?, de Gruyter GmbH, 2017, at p. 19.

[37] See Elizabeth Dwoskin, Craig Timberg, Google now knows when its users go to the store and buy stuff, May 23,

Measurement) matches goods, which are purchased in traditional stores, to the "clicking" of online ads ("Bricks to Clicks"). Thus, the firm is aware of whether a consumer bought the product, on the ad of which she clicked[38].

Another good example is Target, a firm which not only collected, but also produced personal data, meaning the information that a consumer was pregnant. This was, actually, true and the very consumer had not known[39].

So, processing of personal data aims, amongst others, at commercial targeting, including direct marketing and advertising[40], or checking (or predicting)[41] people's characteristics, such as trustworthiness, creditworthiness or identity.

2017, The Washington Post, available at https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?utm_term=.b97032baeb8b.

[38] In 2017, the Electronic Privacy Information Center (EPIC) asked the Federal Trade Commission (FTC) to examine lawfulness of Google's program. See Brian H. Lam and Cynthia J. Larose, United States: FTC Asked To Investigate Google's Matching Of Bricks To Clicks, September 25, 2017, Mondaq, available at http://www.mondaq.com/article.asp?articleid=630914&email_access=on&chk=2167746&q=1536832. It is worth noting that, very recently, Google reported that, in 2017, it took down more than 3.2 billion ads that violated its advertising policies. This included 79 million ads, which aimed to send people to malware-laden sites, 66 million "trick-to-click" ads, and 48 million ads, which attempted to get people to install unwanted software. Google also reported that it blocked 320,000 publishers and blacklisted about 90,000 websites and 700,000 mobile apps for violating Google's policies. See Scott Spencer, An advertising ecosystem that works for everyone, Google, Mar. 14, 2018, available at https://blog.google/topics/ads/advertising-ecosystem-works-everyone/.

[39] Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, Boston College Law Review, Vol. 55, Issue 1, 2014, pp. 94-95, at p. 98. It should be noted that examples of sensitive data processing are not few. See, for example, Jeffrey A. Dretler, United States: Collection Of Biometric Data Raises Privacy Concerns For Employees And Compliance Issues For Employers, March 16, 2018, Mondaq, available at http://www.mondaq.com/article.asp?articleid=683572&email_access=on&chk=2220404&q=1536832; Matt Rosoff, Facebook is facing its biggest test ever—and its lack of leadership could sink the company, March 18, 2018, CNBC, available at https://www.cnbc.com/2018/03/18/facebook-failing-zuckerberg-and-sandberg-absent-commentary.html?utm_source=pocket&utm_medium=email&utm_campaign=pockethits; Daphne Keller, Data Analytics, App Developers, and Facebook's Role in Data Misuse, March 20, 2018, Stanford Law Scholl, available at https://law.stanford.edu/2018/03/20/data-analytic-companies-app-developers-facebooks-role-data-misuse/; Thibaut D'hulst, Van Bael & Bellis, Belgium: Brussels Court Finds Facebook Cookies In Breach Of Data Protection Laws And Imposes € 250,000 Daily Penalty To End Infringement, Mondaq, March 27, 2018, available at http://www.mondaq.com/article.asp?articleid=686834&email_access=on&chk=2223666&q=1536832; Jennifer Kulynych & Henry T. Greely, Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights with Research when Privacy and Science Collide, 3 Journal of Law and the Biosciences, January 15, 2017, pp. 94-132, at p. 119 (mentioning that "[…] *the federal HIPAA Privacy Rule permits entities covered by the Privacy Rule (most health care providers, insurers, and pharmacies) to use or share identifiable patient information without consent to provide treatment. Covered entities may also use identifiable patient information internally, without consent, as necessary to conduct normal business operations* […] *the Privacy Rule also permits 'covered entities' to disclose or share patient information, also without consent, with other covered entities for treatment or reimbursement purposes, and with vendors and contractors who sign an agreement* […]"), available at https://law.stanford.edu/publications/clinical-genomics-big-data-and-electronic-medical-records-reconciling-patient-rights-with-research-when-privacy-and-science-collide/.

[40] See, for example, recent Youtube's practices with regard to advertising: Chaim Gartenberg, YouTube plans to annoy music listeners into subscribing by playing more ads, 'Frustrate and seduce' users into signing up, The Verge, March 21, 2018, available at https://www.theverge.com/platform/amp/2018/3/21/17147800/youtube-streaming-service-lyor-cohen-ads-music-industry-spotify-free.

[41] See Alessandro Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review, Volume 32, Issue 2, April 2016, 238-255, pp. 239-240 (with further references).

To do so, people are profiled and sorted into groups[42] and, thus, further discrimination[43] issues are raised[44].

Setting aside the above practices and risks, let us now move on to social networks' environment to examine the extent, to which people value their privacy, and study some motivations that encourage us to share personal information.

3. The Hedonic Use of (and Several Theories on) Social Networks

Social networks, such as Facebook or Twitter, look for ways to collect a huge volume of data that relate to individuals' online behavior. The more accurate the data collected, the more effective the targeted advertising efforts, which are to be fueled[45]. Such networks' large bases of users are, in fact, very active and check the relevant websites many times a day[46]. For instance, with regard to Facebook[47], approximately 1.4 billion users were daily active for December 2017, while, as of December 31, 2017, 2.13 billion were reported as monthly active users. Moreover, this smart[48] new world[49], in which we

[42] Sorting or profiling may aim, not only to project the "perfect ad", but also to promote the appropriate good at the appropriate price, or to predict criminal behaviors, or to evaluate the accused before sentencing courts. See Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, April 2, 2013, p. 46; Joseph Turow & Lee McGuigan, Retailing and Social Discrimination: The New Normal?, in Seeta Peña Gangadharan (ed.), Data and Discrimination: Collected Essays, 2014, pp. 27-29; Anupam Chander, The Racist Algorithm?, Michigan Law Review, Vol. 115, Issue 6, 2017, p. 1026; State v. Loomis, 881 N.W.2d 749 (Wis. 2016), available at https://harvardlawreview.org/2017/03/state-v-loomis/.

[43] Given correlation that Big Data encourages, firms are aware of e.g. a user's gender (or address, or illness from which she suffers, or her marital status and so forth) and may, thus, discriminate against her -by sorting or profiling- on the grounds of the above personal information. See, amongst others, Danah Boyd & Kate Crawford, Six Provocations for Big Data, A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford Internet Institute, September 21, 2011, available at SSRN: https://ssrn.com/abstract=1926431 or http://dx.doi.org/10.2139/ssrn.1926431; Omer Tene & Jules Polonetsky, Big Data for All, id, at p. 240; Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, International Data Privacy Law, Vol. 3, No. 2, 2013, at p. 76; Cathy O'Neil, Weapons of Math Destruction, How Big Data Increases Inequality and Threatens Democracy, 2016/2017, Broadway Books, NY, pp. 3-5, 130-134, 151.

[44] Oscar Gandy, Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems, Ethics and Information Technology, March 2010, Volume 12, Issue 1, pp. 29-42. Available at https://link.springer.com/article/10.1007/s10676-009-9198-6. For proposals on machine learning systems designing to limit discrimination, see Michael Veale & Reuben Binns, Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data (October 27, 2017), Big Data & Society 4(2), doi:10.1177/2053951717743530. Available at SSRN: https://ssrn.com/abstract=3060763. See also Trevor Hastie, Robert Tibshirani & Jerome Friedman, The Elements of Statistical Learning: Data Mining, Inference, and Prediction, 2nd Edition, 2009, Springer Series in Statistics, available at https://web.stanford.edu/~hastie/Papers/ESLII.pdf.

[45] For instance, algorithms suggest friends etc, and, thus, firms need accurate data to make "good suggestions".

[46] See Maeve Duggan, Nicole B. Ellison, Cliff Lampe, Amanda Lenhart, Mary Madden, Social Media Update 2014, Pew Research Center, January 2015, available at http://www.pewinternet.org/files/2015/01/PI_SocialMediaUpdate20144.pdf.

[47] See stats in Facebook's newsroom, available at https://newsroom.fb.com/company-info/.

[48] Put simply, "smart" implies the addition of three capabilities; sensors, computational power and network communications. See Commission Nationale De L' Informatique Et Des Libertés (CNIL), 36th Activity Report, 2015, id, at p. 35 ("From connected devices to autonomous devices: What freedoms subsist in a robotised world?").

[49] Indeed, it is not only computers that are connected to the Internet, but also many objects communicate with each other in the environment of the Internet of Things. In this context, objects are connected to information networks. For instance, Radio-Frequency Identification enables wireless data collection by readers from electronic tags attached to or embedded in objects –or even people. See Pagnattaro Marisa-Anne, Getting Under Your Skin – Literally: RFID in the Employment Context, Journal of Law, Technology and Policy, No. 2, 2008, pp. 237-257, at p. 238. Available at SSRN: https://ssrn.com/abstract=1565491. Moreover, the so called "smart grid" delivers electricity to consumers by using two-way digital technology to carry, not only electricity but also, information to and from peoples' houses. See Quinn Elias Leake and Reed Adam, Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act (June 16, 2010). University of Colorado Law Review, Vol. 81, 2010, pp. 833-892. Available at SSRN: https://ssrn.com/abstract=1625977. Such technologies may monitor individuals' activities in their home by collecting data, which may relate to vacation time or even caffeine consumption. See Ann Cavoukian, Jules Polonetsky, Christopher Wolf, Smart Privacy for the Smart Grid: embedding privacy into the design of electricity conservation,

are living, encourages users to visit such websites more than ten times per day[50]. As many authors argue, privacy attitudes may quite often be in stark contrast with privacy behaviors[51] and this could be explained by powerful hedonic motivations[52], which encourage users to share their information.

Indeed, social networks can be understood as "hedonic information systems", meaning that their primary goal is self-fulfillment that enables users to experience fun[53]. In this context, people use networks for hedonic purposes[54], such as sharing information and personal data –like personal images– or playing games, watching movies, and so forth. Thus, this use may relate to gratification, meaning escapism or fantasy, social interaction, achievement or self-presentation[55] (and, thus, recognition).

Others support the social capital theory, in accordance with which mutual support, shared norms, social trust and sense of mutual obligations could be detected in social networks[56]. Social capital could, in fact, be understood as the value that an

---

Identity in the Information Society, August 2010, Volume 3, Issue 2, Springer Link, pp. 275–294, available at https://link.springer.com/article/10.1007/s12394-010-0046-y. With regard to the increasing market of robots, which seem to appear in every home, see Calo Ryan, Robots and Privacy, April 2, 2010, Robot Ethics: The Ethical and Social Implications of Robotics, Patrick Lin, George Bekey, and Keith Abney, eds, Cambridge: MIT Press. Available at SSRN: https://ssrn.com/abstract=1599189. See also Bill Gates, A Robot in Every Home, February 1, 2008, Scientific American, available at https://www.scientificamerican.com/article/a-robot-in-every-home-2008-02/.

[50] Subbaraman Nidhi, Smartphone users check Facebook 14 times a day, study says, NBC News, Mar. 28, 2013. Available at https://www.nbcnews.com/tech/tech-news/smartphone-users-check-facebook-14-times-day-study-says-f1C9125315.

[51] See Alessandro Acquisti, Ralph Gross, Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, International Workshop on Privacy Enhancing Technologies, PET 2006: Privacy Enhancing Technologies, Springer Link, pp. 36-58, available at https://link.springer.com/chapter/10.1007%2F11957454_3.

[52] Social networks provide strong hedonic motivations, which can overwhelm and suppress privacy protective behaviors that one may expect in another context. See Parameswaran, M., Whinston, A.B., Research issues in social computing, Journal of the Association of Information Systems, Volume 8, Issue 6, 2007, pp. 336-350. Available at https://www.scopus.com/record/display.uri?eid=2-s2.0-58149460231&origin=inward&txGid=d8a24223ee2ae1b26c9d309cc6e5b676.

[53] See Hans van der Heijden, User Acceptance of Hedonic Information Systems, MIS Quarterly, Vol. 28, No. 4 (Dec., 2004), Management Information Systems Research Center, University of Minnesota, pp. 695-704, at p. 695. Available at https://www.jstor.org/stable/pdf/25148660.pdf (mentioning that "[...] *Hedonic information systems aim to provide self-fulfilling rather than instrumental value to the user, are strongly connected to home and leisure activities, focus on the fun-aspect of using information systems, and encourage prolonged rather than productive use* […]").

[54] See Luqman A., Cao X., Ali A., Masood A., Yu L., Do you get exhausted from too much socializing? Empirical investigation of Facebook discontinues usage intentions based on SOR paradigm, Computers in Human Behavior, 70 (2017), pp. 544-555, available at https://www.researchgate.net/publication/312403527_Do_you_get_exhausted_from_too_much_socializing_Empirical_investigation_of_Facebook_discontinues_usage_intentions_based_on_SOR_paradigm (mentioning that "[...] *Hedonic use of social media is based on the use of SNS for entertainment by* […] *watching movies, sharing experiences with other online users, viewing pictures, playing games with other users, and other forms of online interactions with others* […]"). See also Brandtzæg, P. B., Heim, J., Why people use social networking sites, International Conference on Online Communities and Social Computing, OCSC 2009: Online Communities and Social Computing, Springer Link, pp. 143-152, available at https://link.springer.com/chapter/10.1007/978-3-642-02774-1_16.

[55] Hongxiu Li, Yong Liu, Xiaoyu Xu, Jukka Heikkilä, Hansvan der Heijden, Modeling hedonic is continuance through the uses and gratifications theory: An empirical study in online games, Computers in Human Behavior, Volume 48, July 2015, Elsevier Ltd, pp. 261-272, at p. 261. Available at https://www.sciencedirect.com/science/article/pii/S0747563215000758.

[56] Huysman M., Wulf V., Social Capital and Information Technology, 2004, MIT Press, Cambridge (where it is mentioned that "[…] *The concept of social capital, or the value that can be derived from social ties created by goodwill, mutual support, shared language, common beliefs, and a sense of mutual obligation, has been applied to a number of fields, from sociology to management. It is only lately, however, that researchers in information technology and knowledge management have begun to explore the idea of social capital in relation to their fields.* […]"). Available at https://mitpress.mit.edu/books/social-capital-and-information-technology.

individual may derive from belonging to a community. Moreover, some authors regard "Ubuntu", the central concept of social and political organization in African philosophy, as a way to understand users' behaviors in social networks[57]. This concept consists of the principles of sharing and caring for one another[58]: To be a human is "*to affirm one's humanity by recognizing the humanity of others and, on that basis, establish humane respectful relations with them*"[59] and "to be" is "to belong"[60]. Ubuntu worldview is a community-based mindset, opposed to Western libertarianism and individualism, and close to communitarianism[61]. It is based on values of intense humanness, caring, and associated values to ensure a happy and qualitative community life in a spirit of family. This means that privacy might be considered as less important from this perspective[62]. Hence, as some authors have observed, an image that is shared in social networks and which shows, for instance, one person close to another could, not raise issues of privacy but, prove such relationships, through which one can feel healthy and achieve self-fulfillment[63].

Furthermore, altruism, as the acts of caring about the well-being of other individuals without any expectations and regardless of any direct benefit to oneself[64], could be found in peoples' behavior, while interacting in social networks. For example, individuals may send (e.g. birthday) virtual gifts to their digital friends or might spend some time to write a decent post on a friend's "wall" –for others to see it and– to "honor" this person. The above actions are, of course, undertaken without the expectance of something in return; the very deed is itself the "reward", the intrinsic enjoyable act that comes from helping others[65].

Finally, reciprocity[66] could also be regarded as an important element of peoples' interaction in social networks. Namely, a "friend request" could be treated as a transaction, a request to trade personal data with the expectation that the "offer" will be accepted. A "status update" could be treated as an attempt, undertaken by an individual, who aims to catch attention. Thus, reputation could motivate people to participate in social networks[67]. One could also argue that competition[68], the

[57] Bottis Maria, Social Networks and Personality II, Media and Communication Law, 2/2012, Nomiki Bibliothiki, Greece, pp. 196-199. Available at https://www.nbonline.gr/journals/8/volumes/249/issues/1067/lemmas/4814586.

[58] Ramose M., Globalization and Ubuntu, in Coetzee, Pieter / Roux, Abraham, 2002, Philosophy from Africa, Oxford University Press, 2nd Edition, pp. 626 – 650, at p. 643.

[59] Rafael Capurro, Information Ethics For and From Africa, Keynote address at the African Information Ethics Conference Pretoria (South Africa), 5th to 7th February 2007, in International Review of Information Ethics (IRIE) (2007). Reprinted in: Journal of the American Society for Information Science and Technology (59 (7): 1-9, 2008). Available at http://www.capurro.de/africa.html. See also in Maria Bottis (ed.), A World for Information Law-Proceedings of the 2nd ISIL 2009, Nomiki Bibliothiki, 2010 (pp. 1-130).

[60] M. Brannigan, Ethics Across Cultures with Power Web Ethics, 2005, McGraw-Hill.

[61] Rafael Capurro, id.

[62] Charles Ess, Lost in translation? Intercultural dialogues on privacy and information ethics. Introduction to special issue on Privacy and Data Privacy Protection in Asia. in Ethics and Information Technology, 2005, 7, pp. 1-6; Rafael Capurro, Privacy, An intercultural perspective, in Ethics and Information Technology, Vol. 7, No. 1, 2005, pp. 37-47.

[63] Bottis Maria, Social Networks and Personality II, id, at p. 199.

[64] Cropanzano R., Mitchell S.M., Social Exchange Theory: An Interdisciplinary Review, Journal of Management, Vol. 31 No. 6, December 2005, DOI: 10.1177/0149206305279602, 2005, Southern Management Association, available at http://journals.sagepub.com/doi/10.1177/0149206305279602, pp. 874-900, at p. 879, mentioning that "[…] *Altruism is a rule whereby we seek to benefit another person even at an absolute cost to ourselves* […]".

[65] See also Krebs D., Empathy and altruism, Journal of Personality and Social Psychology, 1975, 32(6), pp. 1134-1146. Available at https://www.ncbi.nlm.nih.gov/pubmed/1214217.

[66] Intention to reciprocate could be regarded as the intention of beneficiary to return help to the benefactors or those who are in the benefactors' group. See Yuanyue Feng, Hua Ye, Why do you return the favor in online knowledge communities? A study of the motivations of reciprocity, Computers in Human Behavior, Volume 63, October 2016, pp. 342-349, available at https://www.sciencedirect.com/science/article/pii/S0747563216303314?via%3Dihub, mentioning that "[…] *reciprocity may also derive from a desire to repay the favor or knowledge received from the community* […] *Such a desire to repay tends to exist in those who frequently obtained necessary information from the communities and learned skills for their tasks* […]".

[67] See also Judith S. Donath, Identity and Deception in the Virtual Community, in Peter Kollock, Marc Smith, Communities in Cyberspace, 1999, Routledge, at p.29, mentioning that "[…] *Identity also plays a key role in motivating people to actively participate in newsgroup discussions* […]".

desire to win in interpersonal situations, could be detected in the above interactions, since people might see it as a pleasure act to e.g. acquire as many friends and followers as possible or to win in games and applications.

Although people may state that they value their privacy, they rarely refuse to share their personal data. Indeed, the above hedonic uses and theories assert that individuals use social network systems to fulfill their need for entertainment or relationships and identity construction. To some, this overrides their privacy concern[69].

So, could there be another way to conceptualize privacy?

4. Negative Conceptualization of Privacy: A Need for Trust and Loyalty

One could argue that trust, as the willingness to accept vulnerability to the actions of others[70], is an essential element of any activity, in which people are involved, such as friendship, commerce, and so forth. Trust can be detected everywhere, since people trust their lawyers or doctors, or that the train will arrive safely to the correct destination. Without trust, politics, commerce and many other fields of everyday life would probably fail. So, could rules be provided to safeguard trust, with regard to privacy policies?

Today, privacy is conceptualized in negative terms. For example, legislators focus on potential harm or data breach, and attention is drawn to the capacity of a person to opt-out. One could argue that privacy is regarded as a "tax on profits", albeit, if trust were incorporated in privacy rules and policies, the latter could encourage information relationships.

As noted above, personal data is collected and processed in ways an individual may not understand or know. This creates confusion and further clouds the image. Thus, it is a problem not only for consumers, but also for governments and firms; when there is no trust, people share less information; when less information is shared, it is hard to achieve economically and socially useful purposes[71].

Under the current regime, rules, which govern personal data, protect –amongst others– interests in informational self-determination[72]. As authors consistently claim, the right to the protection of personal data refers to control over –the processing of– personal data[73]. Thereafter, the key tool for successfully and effectively exercising control is the subject's consent[74] to the above processing.

---

[68] "Competition" means a struggle or contention for superiority and in the commercial world this means a striving for the custom and business of people in the market place: competition has been described as a process of rivalry between firms seeking to win customers' business over time. See Richard Whish, David Bailey, Competition Law, 8th Edition, Oxford University Press, 2015, at p. 4; UK Merger Assessment Guidelines (at para 4.1.2).

[69] Yolanda Jordaan, Gene Van Heerden, Online privacy-related predictors of Facebook usage intensity, Computers in Human Behavior, Volume 70, May 2017, pp. 90-96. Available at https://www.sciencedirect.com/science/article/pii/S0747563216308767?via%3Dihub.

[70] For several definitions of "trust", see also Ethan J. Leib, Friends as Fiduciaries, 86 Wash. U. L. Rev. (2008-2009), pp. 665-732, at p. 693 (mentioning, amongst others, that "[…] *Trust is accepted vulnerability to another's power to harm one, a power inseparable from the power to look after some aspect of one's good* […]"). Available at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1089&context=faculty_scholarship.

[71] Indeed, data processing is essential for crucial purposes, such as health care, education, commerce, crime detection or terrorism prevention. See Corien Prins, Property and Privacy: European Perspectives and the Commodification of our Identity, in L. Guibault and P.B. Hugenholtz (eds), The Future of the Public Domain, Identifying the Commons in Information Law, 2006, Kluwer Law International, pp. 226-230. See also Bartha Maria Knoppers, Adrian Mark Thorogood, Ethics and Big Data in health, Big data acquisition and analysis, Current Opinion in Systems Biology, 2017, Vol. 4, pp. 53-57, at p. 53, who argue that the right to science could be activated to achieve free movement of data that would, in turn, benefit human kind.

[72] Maria Bottis, Law and information: a "love-hate" relationship, in Maria Bottis (ed.), The history of Information: From papyrus to the electronic document, id, pp. 141-152, at p. 148; Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke & Mark Hansen, Self-Surveillance Privacy, Iowa Law Review, vol. 97:809, 2012, pp. 809-847, at p. 820.

[73] See, amongst others, Manon Oostveen & Kristina Irion, The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right? University of Amsterdam, Institute for Information Law, Paper No. 2016-06.

[74] "[…] *If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing* […]" (Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, 01197/11/EN/WP187). See also Omer Tene & Jules Polonetsky, Big Data for All, id, pp. 260-263; Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review, Vol. 126:1880,

This concept of control and consent focuses on the harm that has to be avoided or the consent that has to be obtained. In this context, some regard social networks' advertising practices as something creepy[75], or speak of "surveillance" that aims to subject individuals to criminal punishment or deny access to health, work and other essential fields[76]. In other words, attention is mainly devoted to harm, rather than opportunities, and, hence, privacy is treated as a negative element that has to be balanced against innovation, efficiency or security.

However, control and privacy self-management is in practice impossible and innumerous jokes on terms of use[77] can prove this. Furthermore, the "choice" to disclose personal data is an illusion; one has no choice to opt-out of profiling by firms, of whose existence she is unaware.

On the other hand, opting-out of the alleged –firms' and governments'– surveillance[78] would mean opting-out of society[79]. So, what if trust were enabled, with regard to privacy laws, to allow people to safely share their personal data for the benefit of both individuals and firms?

Trust is the key element of healthy relationships and societies[80]. It has been defined as a willingness to rely on another, and, in particular, as "*a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another*"[81]. To put it simply, trust is a state that enables an individual to be willing to make herself vulnerable to another party, to rely on another, despite potential risks –that the latter will act in a way that can harm the former[82].

2013, p. 1894.

[75] See, for example, Caitlin Dewey, 9 Answers About Facebook's Creepy Emotional-Manipulation Experiment, The Washington Post (July 1, 2014), available at https://www.washingtonpost.com/news/the-intersect/wp/2014/07/01/9-answers-about-facebooks-creepy-emotional-manipulation-experiment/?utm_term=.8443bd9a9c59. See also Omer Tene, Jules Polonetsky, A Theory of Creepy: Technology, Privacy, and Shifting Social Norms, Yale Journal of Law and Technology, Vol. 16, Iss. 1, Article 2, 2014, pp. 59-102, available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1098&context=yjolt; Danah Boyd, Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence, Convergence: The International Journal of Research into New Media Technologies, London, Los Angeles, New Delhi and Singapore Vol 14(1), pp. 13-20, DOI: 10.1177/1354856507084416, available at http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf.

[76] See Joseph Turow & Lee McGuigan, Retailing and Social Discrimination: The New Normal?, id; Anupam Chander, The Racist Algorithm? id; State v. Loomis, 881 N.W.2d 749 (Wis. 2016), id.

[77] See, amongst others, Simon Chesterman, Privacy and Our Digital Selves, September 7, 2017, The Straits Times, September 2, 2017, available at SSRN: https://ssrn.com/abstract=3033449 (at p. 3, mentioning that "[…] *The British retailer GameStation gave us memorable proof of this one April Fool's Day, when more than 7,000 people clicked "I accept" to terms and conditions that included the surrender of their immortal souls to the company. (The company later rescinded all claims, temporal and spiritual)* […]"). See also Alexis Madrigal, Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days, The Atlantic (Mar. 1, 2012), available at https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[78] See, amongst others, Parker Higgins, Big Brother Is Listening: Users Need the Ability to Teach Smart TVs New Lessons, The Electronic Frontier Foundation, Feb. 11, 2015, available at https://www.eff.org/deeplinks/2015/02/big-brother-listening-users-need-ability-teach-smart-tvs-new-lessons.

[79] See, in general, Julia Angwin, Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance, 2015, S. Martin's Griffin Edition.

[80] See, amongst others, Francis Fukuyama, Trust: The Social Virtues and The Creation of Prosperity, Free Press Paperbacks, 1996, USA.

[81] Denise M. Rousseau, Sim B. Sitkin, Ronald S. Burt, Coun Camerer, Introduction to special topic forum not so different after all: A cross-discipline view of trust, Academy of Management Review, 1998, Vol. 23, No. 3, pp. 393-404, at pp. 394-395. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.8322&rep=rep1&type=pdf.

[82] In commercial relationships, trust begins with the promise that leads to a contract. A contract is, in turn, the most important tool and a mechanism to encourage trust. See, amongst others, Eli Bukspan, Trust and the Triangle Expectation Model in Twenty-First Century Contract Law, 11 DePaul Bus. & Com. L.J., 2013 pp. 379-415, at pp. 382-383. Available at: http://via.library.depaul.edu/bclj/vol11/iss3/4. In fields of personal relationships, the quality of a friendship depends on the extent of trust between people. See Irwin Altman, Reciprocity of Interpersonal Exchange,

In the context of privacy, trust would mean the willingness to become vulnerable to a person or entity by sharing personal data. In this case, the party (individual), who discloses her information, would be the "trustor"[83], the act of disclosing data would be the "entrusting", and the recipient of the data would be the "entrustee"[84]. Indeed, in present-day societies, we are all "trustors", since we entrust firms, when disclosing information to, for instance, a search engine or any other digital firm. Furthermore, one becomes vulnerable, when she faces the risk of misuse or unauthorized disclosure of her data. Namely, vulnerability may refer to the potential risk of an employee being fired, or the risk of selling data to third parties.

If the concept of trust were introduced in privacy regime and laws, it could further enable honesty and loyalty. This could be achieved through flexible fiduciary[85] laws[86], the main goal of which is to protect against exploitation of a vulnerability created by trusting another[87]. Hence, these rules impose duties of loyalty and care. In particular, a fiduciary is a person who has a relationship of trust with a party –the beneficiary– and who is authorized to hold something valuable (for instance, the beneficiary's assets) and manage them on the beneficiary's behalf[88]. So, fiduciary laws could, indeed, apply in a flexible way[89] to protect individuals. Moreover, an affirmative obligation of honesty could be introduced, since fiduciaries have duties of disclosure, care and loyalty, while they are also obliged to keep the beneficiary informed[90].

This way, individuals (as beneficiaries) would very likely, not only know what information would be disclosed but also, understand both information and processing techniques. Furthermore, firms (as fiduciaries) could very well be obliged to

---

Journal of the theory of social behavior, Volume3, Issue 2, October 1973, pp. 249-261. Available at https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-5914.1973.tb00325.x. So, maybe this is the reason why people share their data in social networks. This could mean that privacy is not just for selfish users but also for people who wish to share data or firms that need users to disclose information.

[83] Fiduciary laws use, amongst others, the term "beneficiary". Other terms, such as "principal" (agency) or "entrustor", may also be used to refer to this party. See Tamar Frankel, Fiduciary Law, California Law Review, Volume 71, Issue 3, Article 1, May 1983, pp. 795-836, at p. 800, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2137&context=californialawreview.

[84] Fiduciary laws use the term "trustee". See Tamar Frankel, Fiduciary Law in the twenty-first century, Boston University Law Review, 2011, Vol. 91, pp. 1289-1299. Available at https://www.bu.edu/law/journals-archive/bulr/documents/frankel.pdf.

[85] The term "fiduciary" comes from the Latin verb "fidere" that means to "trust". Fiduciary duty is a legal term that refers to the type of duty that a person or organization, who manages someone else's wealth or property, has in certain circumstances in relation to the owner or beneficiary of that wealth or property. So, fiduciary duties are legal obligations that exist in certain situations between one party (the beneficiary) that owns or has the rights to assets that another party (the fiduciary or trustee) manages. See The European Commission, Resource Efficiency and Fiduciary Duties of Investors, Final Report, ENV.F.1/ETU/2014/0002, DG Environment, at p. 22. Available at http://ec.europa.eu/environment/enveco/resource_efficiency/pdf/FiduciaryDuties.pdf.

[86] One of the most important fiduciary duties is the duty of loyalty, meaning that fiduciaries should act in good faith in the interests of their beneficiaries and impartially balance the conflicting interests of different beneficiaries. They should avoid conflicts of interest and should not act for the benefit of themselves or a third party. Another important duty is the duty to act prudently, which means that fiduciaries should act with due care, skill and diligence. See The European Commission, Resource Efficiency and Fiduciary Duties of Investors, id, at p. 7. The concept of fiduciary duty is present in the legislation of every EU Member State. See The European Commission, Resource Efficiency and Fiduciary Duties of Investors, id, at p. 8; UNEP FI, 2005, A Legal Framework for the Integration of Environmental, Social and Governance Issues into Institutional Investment. UNEP Finance Initiative and Freshfields Bruckhaus Deringer.

[87] Ethan J. Leib, Friends as Fiduciaries, id, at p. 732, arguing that fiduciary laws are set up specifically to give effect to and frame this specific relationship of trust and vulnerability.

[88] Jack Balkin, Information Fiduciaries in the Digital Age, 2014. Available at https://balkin.blogspot.nl/2014/03/information-fiduciaries-in-digital-age.html.

[89] The understanding and implementation of fiduciary duties are dynamic and constantly evolving in response to changes in society, economy and knowledge. See The European Commission, Resource Efficiency and Fiduciary Duties of Investors, id, at p. 22. See also Ethan J. Leib, Friends as Fiduciaries, id, at pp. 707, 732 (supporting flexibility of fiduciary laws).

[90] See Frank H. Easterbrook, Daniel R. Fischel, Contract and fiduciary duty, The Journal of Law and Economics, The University of Chicago Law School, Vol. XXXVI, April 1993, pp. 425-446, at p. 445. Available at https://www.jstor.org/stable/pdf/725483.pdf?refreqid=excelsior:f0dcfbefabd109b7c791dbde37cdb31f.

consult with individuals (their beneficiaries) and give them the opportunity to express their "best interests" (or even opinions) in accordance with which data would be shared[91]. Maybe such rules could oblige firms to implement internal policies and other safeguards, such as employee training. Contracts to forbid e.g. re-identification of anonymized[92] data might also be introduced. If this were the case, trust would be enhanced and, thus, more information would be safely disclosed for the benefit of both firms and humans.

Fiduciary laws are, indeed, flexible and could, thus, apply to processing of personal data. One more reason to be very optimistic, with regard to the above potential to enhance trust, is the novelty introduced by the GDPR: the right to data portability.

5. The Right to Data Portability: a Novelty and a Potential to Enhance Trust

One of the most important rights that the GDPR introduces is the right to data portability[93]. Under Article 20 of the GDPR, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided[94] to a controller, in a structured, commonly used and machine-readable format[95] and have the right to transmit those data to another controller without hindrance[96] from the controller to which the personal data have been provided, where the processing is based on consent or on a contract, and where the processing is carried out by automated means[97]. While data subjects exercise their right to data portability they should have the right to have the personal data transmitted directly

[91] See J. Sandberg, Socially Responsible Investment and Fiduciary Duty: Putting the Freshfields Report into Perspective, Journal of Business Ethics, 101, Springer 2010, DOI 10.1007/s10551-010-0714-8, pp. 143–162, at p. 157. Available at https://link.springer.com/content/pdf/10.1007%2Fs10551-010-0714-8.pdf.

[92] As many authors argue, in the age of Big Data there is no manner in which to render personal data anonymous, due to the fact that the ("anonymized") data subject is in any case identifiable. See, amongst others, Bruce Schneier, Data and Goliath, The Hidden Battles to Collect Your Data and Control Your World, 2015, W.W. Norton & Company, pp. 50-53; Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of anonymization, UCLA Law Review, 2010, University of Colorado, Law Legal Studies Research Paper No. 9-12, Vol. 57, p. 1701; Latanya Sweeney, Simple demographics often identify people uniquely, Carnegie Mellon University, 2000, Data Privacy Working Paper No. 3; Philippe Golle, Revisiting the uniqueness of simple demographics in the US population, 5th ACM Workshop on Privacy in the Electronic Society (WPES'06), 2006; Melissa Gymrek et al., Identifying personal genomes by surname inference, Science NY, 2013, Vol. 339, Issue 6117, pp. 321-324, doi: 10.1126/science.1229566 (available at http://science.sciencemag.org/content/339/6117/321.long); John Bohannon, Genealogy databases enable naming of anonymous DNA donors, Science NY, Jan. 18, 2013, Vol. 339 (available at http://www.johnbohannon.org/NewFiles/DNA_privacy.pdf); Arvind Narayanan & Vitaly Shmatikov, Robust de-anonymization of large sparse datasets, May 18-22, 2008, IEEE Symposium on Security and Privacy, Oakland, CA, USA, DOI: 10.1109/SP.2008.33 (available at http://ieeexplore.ieee.org/document/4531148/).

[93] The term "portability" can be detected in previous provisions. For instance, Article 30 of the Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) mentions the "number portability", which relates to the right of all subscribers of publicly available telephone services to retain their number(s). See also Recital (31) of the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[94] Data "provided by" an individual includes personal data that relates to a person's activity or that comes as a result from observation. See Article 29 Data Protection Working Party, Guidelines on the right to data portability, Adopted on 13 December 2016 (as last Revised and adopted on 5 April 2017), at pp. 9-10.

[95] Under Recital (21) of the Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information "[…] *A document should be considered to be in a machine readable format if it is in a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it* […]".

[96] Such "hindrance" can be characterized "*as any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller*". See Article 29 Data Protection Working Party, Guidelines on the right to data portability, id, at p. 15 (where it is mentioned that such hindrance could be fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demands).

[97] See Article 20(1) of the GDPR. See also Recital (68) of the GDPR.

from one controller to another, where technically feasible[98].

The right to data portability[99] can be regarded as an economic right, which aims to let individuals "share wealth" created by new technologies[100] and benefit from digital services. One of its purposes is to create a competitive market environment that will enable consumers to switch providers[101]. The above right, however, aims, not only to enforce competition and consumer protection but also, to promote interconnection of services and interoperability[102]. Hence, user-centric platforms could be introduced and developed for the benefit of individuals' interests[103]. So, the right to data portability is not just an economic right, but it also aims to enhance individuals' rights[104] and promote transparency and minimization of unfair and discriminatory practices[105].

---

[98] See Article 20(2) of the GDPR. Under Article 20(3-4) of the GDPR "[…] *The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.* […] *The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others* […]". See also Recital (68) of the GDPR ("[…] *The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another* […]").

[99] For a discussion with regard to origins of the right to data portability (i.e. the users' need to transfer data that they had been building up, such as e-mail, friends' lists or address books from one service to another), see Barbara Van der Auwermeulen, How to attribute the right to data portability in Europe: A comparative analysis of legislations, Computer Law & Security Review 33 (2017), pp. 57–72, at p. 58, available at https://www.sciencedirect.com/science/article/pii/S0267364916302175.

[100] See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014, at p. 47.

[101] See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, under Article 7 of Directive 95/46/EC, id, at p. 48, which further mentions that "[…] *it can also contribute to the development of additional value-added services by third parties who may be able to access the customers' data at the request and based on the consent of the customers. In this perspective, data portability is therefore not only good for data protection, but also for competition and consumer protection* […]".

[102] Interconnection and interoperability among different products require agreed-upon interfaces and specifications, which are called "standards". Some standards may emerge from market usage (like those applicable to screw drivers). Others are "proprietary standards" and are established by a small group of firms that develop the standards and, then, try to enlist commercial support for them. Finally, some standards (such as that of Wi-Fi) evolve from the work of Standard Setting Organizations (SSOs), like the Institute of Electrical and Electronics Engineers (IEEE). See D. Melamed, R. Picker, P. Weiser, D. Wood, Antitrust Law and Trade Regulation, Cases and Materials, 7th Edition, 2018, Foundation Press, at p. 927. See also Article 29 Data Protection Working Party, Guidelines on the right to data portability, id, at p. 3, mentioning that "[…] *the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers. It will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy* […]".

[103] See Article 29 Data Protection Working Party, Guidelines on the right to data portability, id, at p. 3.

[104] See Recital (68) of the GDPR ("[…] *To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller* […]").

[105] See Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, at p. 47.

This new right is a unique opportunity, with regard to competition law[106] and business practices[107], while at the same time –and most importantly– it will very likely help increase trust[108] and transparency[109], promote innovation[110], and turn passive data subjects into active re-users[111], who will, indeed, share wealth that new technologies create[112].

For instance, thanks to this novelty, users could provide their data, without the need to manually add it to each new service or platform. While individuals would add or change their information, this would be updated on other services, without the need to visit other platforms to re-enter it. Firms would receive such data and there would be no need to "fill forms", a factor that could drive people away. At the same time, individuals would share experiences, and their data could be automatically updated on a provider's service, if the data subject permitted it. Thus, relationship between users and providers would not only remain up-to-date but also encourage continuous usage. Thereafter, mutual benefit could be achieved.

6. Discussion

In other fields of law, authors have proposed[113] the introduction of trust to overcome weaknesses with regard to missing, inadequate, or inaccurate information. For instance, concerning biobanks, information provided to donors, relating to secondary uses of samples, is inadequate. Trust could, thus, be introduced to develop a new model of consent, where healthcare providers, researchers, patients, and participants could consult. Such consultation could reshape classic models of "informed consent" and values could be communicated between healthcare providers and researchers, while patients' choices would very likely be activated. A more realistic and applicable model could, hence, be developed for cases, in which access to information is denied or information is inadequate –and providing an "informed consent" is impossible. This model would reconstruct relationships between patients, participants, healthcare providers, and researchers, and values of trust and reciprocity could be introduced. In this context, decision making process would probably focus on patients and their needs. For the above reasons, some authors[114] regard the "model of trust" as a more appropriate way to

[106] See I. Graef, J. Verschakelen, P.Valcke, Putting the Right to Data Portability into a Competition Law Perspective (2013), Law: The Journal of the Higher School of Economics, Annual Review, 2013, pp. 53–63. Available at https://lirias.kuleuven.be/bitstream/123456789/447770/1/HSE+Law+Journal+-+Putting+the+right+to+data+portability+in+a+competition+law+perspective.pdf.

[107] See D. Geradin & M. Kuschewsky, Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue, February 12, 2013. Available at SSRN: https://ssrn.com/abstract=2216088 or http://dx.doi.org/10.2139/ssrn.2216088, at pp. 9-10.

[108] See E. Bizannes, Why Every Site Should Have Data Portability Policy, Techcrunch, June 23, 2010, available at https://techcrunch.com/2010/06/23/data-portability-policy/, mentioning that sites and their users have a relationship, and the relationship is stronger if the user can trust the website to protect their domain over their data.

[109] See European Data Protection Supervisor, Opinion 9/2016, Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data, at p. 13, par. 55, available at https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf; Article 29 Data Protection Working Party, Guidelines on the right to data portability, id, at p. 15.

[110] See Article 29 Data Protection Working Party, Guidelines on the right to data portability, id, at p. 5.

[111] See B. Custers. H. Ursic, Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection, International Data Privacy Law, January 7, 2016, at p. 9. Available at http://data-reuse.eu/wp-content/uploads/2016/01/International-Data-Privacy-Law-2016-Custers.pdf.

[112] See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, under Article 7 of Directive 95/46/EC, id, at p. 47.

[113] See Giuseppe Schiavone, Gabriele De Anna Matteo Mameli, Vincenzo Rebba, Giovanni Boniol, Libertarian paternalism and health care policy: a deliberative proposal, Medicine, Health Care and Philosophy, Volume 17:1 (2014), pp. 103-113, available at https://link.springer.com/article/10.1007%2Fs11019-013-9502-4; Rebecca Dresser, "Right to Try" Laws: The Gap between Experts and Advocates, Hastings Center Report Vol. 45:3 (2015), pp. 9-10, available at http://onlinelibrary.wiley.com/doi/10.1002/hast.442/abstract; Virginia Sanchini, Giuseppina Bonizzi, Davide Disalvatore, Massimo Monturano, Salvatore Pece, Giuseppe Viale, Pier Paolo Di Fiore, Giovanni Boniolo, A Trust-Based Pact in Research Biobanks. From Theory to Practice, Bioethics, Vol. 30:4 (2015), pp. 260–271. DOI: 10.1111/bioe.12184, available at http://onlinelibrary.wiley.com/wol1/doi/10.1111/bioe.12184/full; Giovanni Boniolo, The Art of Deliberating, Democracy, Deliberation and the Life Sciences between History and Theory, Verlag Berlin Heidelberg, Springer, 2012, pp. 1-44, available at https://link.springer.com/content/pdf/10.1007/978-3-642-31954-9.pdf.

approach consent –and overcome weaknesses relating to inadequate or inaccurate information.

Similar proposals have been submitted to effectively and successfully exercise the –American– "right to try"; a right that allows terminally ill patients to request access to early stage experimental medical products, such as drugs or experimental treatments, directly from the producer, removing the approval of the Food and Drug Administration[115]. Justifications for the above right (to try) laws are based on the ethical principles of autonomy, beneficence and justice[116].

These proposals could very well constitute a prescription for the implementation of flexible solutions and the activation of mechanisms in other fields, where consent of the individual plays an important role in examining whether specific procedures are lawful. In particular, after having studied personal data processing practices that firms conduct, several risks and dangers were detected[117]. Moreover, users' behaviors in social networks revealed that, while individuals may believe that they value their privacy, albeit, they often disclose a huge volume of personal data on a daily basis. Current negative conceptualization of privacy calls for a positive approach by introducing the concept of trust to safeguard individuals' rights and interests. This could be achieved by applying flexible fiduciary laws, in conjunction with the promising new right to data portability.

Indeed, re-shaping current European privacy model could be a welcome proposal; it is not only a model that has been regarded as "the triumph of individualism"[118], where consent may abrogate the unjust nature of data processing (a processing, which is by definition unlawful), but it is also a model that permits consent to be given by "a single-mouse-click" on terms of use, i.e. by ticking a box in a website[119]. If trust were introduced, such contradictions would probably be avoided.

In present-day societies, the protection of privacy may not relate that much –or may not relate just– to the "*right to be let alone*", which Warren and Brandeis[120] defined many years ago. Maybe, it relates more –or relates especially– to trust and loyalty that shall govern relationships between firms and individuals.

Perhaps, trust should be implemented in the European model of privacy, where "consent" is 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*"[121], to add values of loyalty and reciprocity in relationships between data subjects and processors. Decision making process could, then, focus on individuals and their needs for transparent processing of personal data for the benefit of the data subjects. This way, individuals would very likely share wealth created by Big Data, while at the same time opaque procedures of data processing would come to an end[122].

---

[114] D. Carrieri, F.A. Peccatori, G. Boniolo, The ethical plausibility of the 'Right To Try' laws, Critical Reviews in Oncology / Hematology Vol. 122 (2018), pp. 64–71. Available at https://ac.els-cdn.com/S1040842817304420/1-s2.0-S1040842817304420-main.pdf?_tid=6b8db204-a2d0-4a33-a162-0581b5e35b3e&acdnat=1522553099_69cfc7b73320bd366e99ee5dd179be75.

[115] D. Carrieri, F.A. Peccatori, G. Boniolo, The ethical plausibility of the 'Right To Try' laws, id, at p. 64.

[116] See also Jennifer Piel, Informed Consent in Right-To-Try Cases, J Am Acad Psychiatry Law Vol. 44 (2016), pp. 290-296. Available at http://jaapl.org/content/jaapl/44/3/290.full.pdf.

[117] See also Jennifer Kulynych & Henry T. Greely, Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights with Research when Privacy and Science Collide, id, at p. 113 (mentioning that patients would be surprised to know that they do not own the medical records that their providers maintain; whether paper or electronic, these records are generally viewed as a business asset owned by the patient's provider). Kulynych and Greely point out that the more scientists learn about genetic profiling, the more this profiling re-identification risk will escalate (Jennifer Kulynych & Henry T. Greely, id, at p. 106). Referring to the need for informed consent and after having observed that medical identity theft is one of the fastest growing and most expensive consequences of healthcare data breach, the above authors argue that technology makes it possible to render every patient an involuntary subject of genomic research (Jennifer Kulynych & Henry T. Greely, id, at pp. 108, 110).

[118] Maria Bottis, The protection of private life and the European legislation with regard to personal data: Thoughts on the protection of private life in the USA, in Stathopoulos M., Honorary Volume, Sakkoulas Publications, Greece, pp. 809-823, at p. 811.

[119] See recital (32) of the GDPR.

[120] S. Warren & L. Brandeis, The Right to Privacy, id.

[121] See Article 4(11) of the GDPR.

[122] With regard to healthcare, some authors treat medical algorithms as a kind of "Black-Box medicine" and argue that

Besides, as personal data subjects, as "owners" of the "fuel" of information economy and societies[123], we are nothing but "patients" in an environment, where access to information has a vital role to play, and where the full enjoyment of wealth resulting from personal data processing –treated, insofar as it is able, as the enjoyment of the results emerging from experimental medical treatments– may constitute a fundamental right derived from the ethical principles of autonomy, beneficence and justice.

So, in response to challenges posed by new technologies, has the time come to implement trust into the European concept of privacy?

individuals should enjoy a right to explanation of decisions made about them by algorithms. See E. Scott Brummel, Confronting natural conflicts of interest and artificial intelligence, Journal of Law and the Biosciences, Volume 4, Issue 2, 1 August 2017, pp.435-444, at pp. 441, 443, available at https://academic.oup.com/jlb/article/4/2/435/4265565. With regard to opaque procedures of data processing, see also: Michael Butterworth, The ICO and artificial intelligence: The role of fairness in the GDPR framework, Computer Law and Security Review, The International Journal of Technology Law and Practice, forthcoming 2018, at p. 3, DOI: 10.1016/j.clsr.2018.01.004, available at https://www.researchgate.net/publication/323465567_The_ICO_and_artificial_intelligence_The_role_of_fairness_in_the_GDPR_framework; Cathy O'Neil, Weapons of Math Destruction, id; Corien Prins, Property and Privacy, id; Chris Jay Hoofnagle, Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, N.C. J. Int'l L. & Com. Reg. Vol. 29 (2003), pp. 595-638, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.gr/&httpsredir=1&article=1677&context=facpubs; Jon D. Michaels, All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror, Cal. L. Rev. Vol. 96:4 (2008), pp. 901-966, available at https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.gr/&httpsredir=1&article=1169&context=californialawreview.

[123] Frank Pasquale, The Black Box Society, The Secret Algorithms that Control Money and Information, England, Harvard University Press, 2015, at p. 141.