14

Big Data and Privacy Fundamentals: Toward a "Digital Skin"

David Manset

We may be witnessing the advent of the era of Big Data, but new regulations, including the European Union's General Data Protection Regulation (GDPR) (European Commission 2012) and EU–US Privacy Shield (European Commission 2016a) will, in the near future, greatly impact the way sensitive data can be accessed, shared, and processed.[1]

This societal evolution will require health-care information systems to make a giant leap toward empowering the "data subject"—you, me,

[1] According to the European Commission, the GDPR will enable people to better control their personal data while modernizing and unifying rules to create a "digital single market" that will "make Europe fit for the digital age" (see: http://europa.eu/rapid/press-release_IP-15-6321_en.htm, accessed October 3, 2016).

The EU–US Privacy Shield is a framework designed to "protect the fundamental rights of anyone in the EU whose personal data is transferred to the United States." It also "(brings) legal clarity for businesses relying on transatlantic data transfers" (see: http://europa.eu/rapid/press-release_IP-16-2461_en.htm, accessed October 3, 2016).

D. Manset (✉)
be-studys, be-almerys, 336 Rue Saint Honore, Paris, France
e-mail: david.manset@almerys.com

L. Menvielle et al. (eds.), *The Digitization of Healthcare*,
DOI 10.1057/978-1-349-95173-4_14

everyone—when it comes to building and sharing an acceptable "quantified self."

This chapter explores the lessons learned in 20 international studies regarding the processing of medical data and the associated legal and technical implications. It concludes with a possible response to the (big) data-protection dilemma in terms of the fundamental principles at stake, and the potential technological paradigms that could support the development of a fair(er) digital economy.

14.1 Introducing the Big Data Dilemma

Our society is undergoing a digital transformation. The health-care and insurance sectors, which serve as foundational pillars for most national systems of government, are moving from silo-based, complex and slow-changing monopolistic and information systems to decoupled, rapidly growing and heterogeneous data landscapes.

Facilitated access to health-care information systems, the reduced cost of genome sequencing, and the unprecedented volume of connected devices now flooding the market are among the many signs of an emerging ubiquitous and interconnected society powered by Big Data.

This globalization is leading us inexorably toward the question of our "quantified self" (Picard and Wolf 2015). In other words: How much personal data should be shared with "society"? What are the associated risks and benefits? What is the actual value of our data, and who owns it? What will this mean for concerned individuals, organizations, and information systems? These are questions that must be pondered with care and scrutinized in terms of good practices and applicable laws (Leonard Kish and Eric Topol 2015).

In the next section, we explore Europe's legal framework, the issues associated with the use of sensitive data and the applicable technologies and new paradigms, and conclude with a look at a set of basic but foundational principles and technologies that enable digital trust.

14.2 Europe's Legal Framework

The legal framework of data protection in Europe builds on a complex and historical regulatory background inscribed in a corpus of bodies, laws, and charters. This is what the following privacy compass (Fig. 14.1) illustrates. It features a 360-degree outlook, together with some of the proposed scientific and technological approaches described in this chapter.

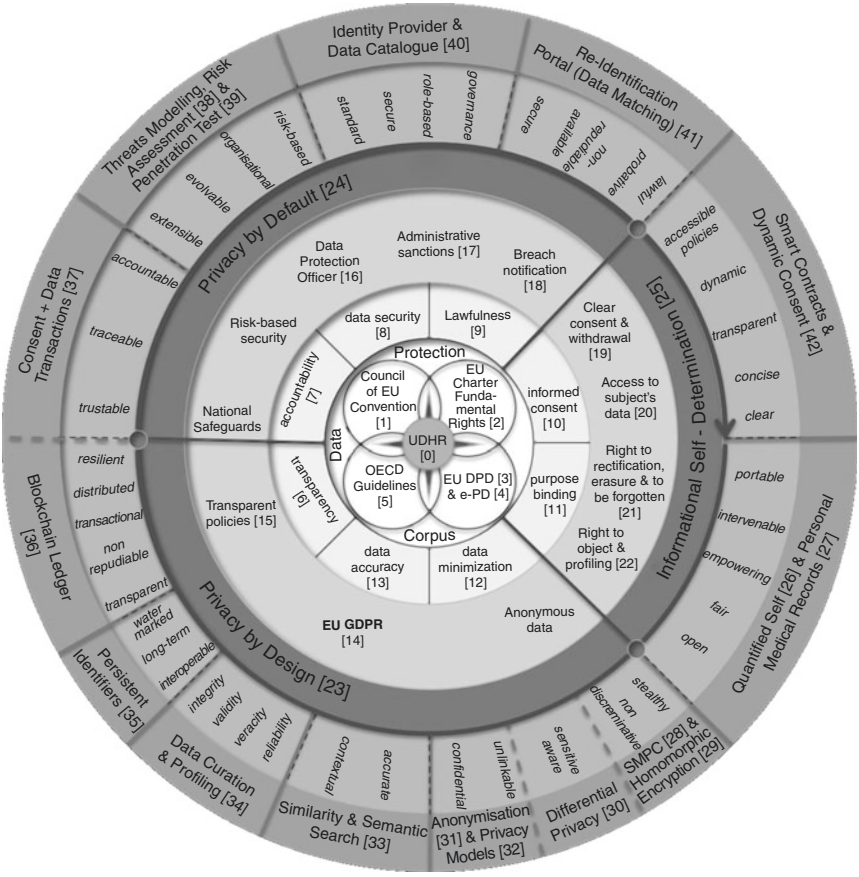

Fig. 14.1 The privacy compass references

(*Continued*)

Fig. 14.1 (continued)

DPD = Data Protection Directive; e-PD = e-Privacy Directive; EU = European Union; GDPR = General Data Protection Regulation; OECD = Organisation for Economic Co-operation and Development; UDHR = Universal Declaration of Human Rights.

[0] Lauterpacht, Hersch. "Universal Declaration of Human Rights, the." Brit. YB Int'l L. 25 (1948): 354.

[1] "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data." *Treaty Office*. Council of Europe, Web. March 28, 2016.

[2] "Abstract of EU: Charter Of Fundamental Rights Of The European Union." *International Legal Materials* 40.2 (2001): 1–265. European Commission. Web. March 28, 2016.

[3] "31995L0046—Directive 95/46/EC." *EUR-Lex*. European Parliament. Web. February 15, 2016.

[4] "32002L0058—Directive 2002/58/EC." *EUR-Lex*. European Parliament. Web. February 15, 2016.

[5] "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)." (n.d.): n. pag. OECD. Web. March 28, 2016.

[6] Ali Gholami, Anna-Sara Lind, Jane Reichel, Jan-Eric Litton, Ake Edlund, Erwin Laure, Privacy Threat Modeling for Emerging BiobankClouds, *Journal of Procedia Computer Science* 37 (2014): 489–496, 493. And EU DPD, Paragraphs 38–40 of the Preamble, Articles 10–15 of the DPD.

[7] Aspects of the principle can be seen, among others, in Art. 17 DPD (Security of processing).

[8] EU DPD. Art. 17 (Security of processing).

[9] EU DPD. Paragraphs 18, 23, 28 of the Preamble, Article 6 of the Data Protection Directive.

[10] EU DPD. Paragraph 30 of the Preamble, Article 7 of the DPD.

[11] EU DPD. Paragraphs 28–31 of the Preamble, Articles 6 and 7 of the DPD.

[12] EU DPD. Paragraphs 59–61 of the Preamble, Articles 16–17 of the DPD.

[13] EU DPD. Paragraphs 28 and 41 of the Preamble of the DPD.

[14] "EU General Data Protection Regulation." European Council, Web. March 28, 2016.

[15] EU GDPR, Art. 11 ("concise, transparent, clear and easily accessible policies"), Art. 15 ("right to access and to obtain data for the data subject").

[16] Art. 5(1) point (f); Art. 22 ("Responsibility and accountability of the controller"); Art. 33 ("Data protection impact assessment"); Art. 35 ("Designation of the data protection officer").

[17] Art. 5(1) point (a) GDPR principles "lawfulness, fairness and transparency," and Art. 6 GDPR "lawfulness of processing."

[18] Cornelia Graf, Peter Wolkerstorfer, Arjan Geven, and Manfred Tscheligi. A pattern collection for privacy enhancing technology. In The 2nd Int. Conf. on Pervasive Patterns and Applications (PATTERNS 2010), Lisbon, Portugal, November 21–26, 2010.

[19] EU GDPR, Art. 13a ("standardised information policies"), Art. 4(8) definition of the "data subject's consent," and Art. 7 "conditions for consent."

[20] EU GDPR, Art. 14 ("information to the data subject").

[21] EU GDPR, Art. 12 (for defining the conditions for exercising data subject rights).

[22] EU GDPR, Article 4(3aa) on data profiling definition and Article 14(1) on profiling-based decision.

[23] Cavoukian, Ann. *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. N.p.: n.p., n.d. Information and Privacy Commissioner, 2012. Web. March 28, 2016. And "7 Foundational Principles—Privacy By Design." Privacy By Design. N.p., n.d. Web. November 11, 2015.

[24] Cavoukian, Ann. *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. N.p.: n.p., n.d. Information and Privacy Commissioner, 2012. Web. March 28, 2016. And "7 Foundational Principles—Privacy By Design." Privacy By Design. N.p., n.d. Web. November 11, 2015

[25] Empowerment: American community psychology, social scientist Julian Rappaport (1981) and Volkszählungsurteil, BVerfGE Bd. 65, S. 1ff. and Some Federal States (Länder) have, in their own Constitutions, made data protection a seperate, independent right: see, e.g., Art. 33 of the Constitution of Berlin.

[26] Wolf, Gary. "The Quantified Self." Antephase RSS. N.p., n.d. Web. November 11, 2015.

[27] "You Should Get to Know You—UnPatients." UnPatients. N.p., n.d. Web. November 11, 2015.

[28] Goldreich, Oded. "Secure multi-party computation." Manuscript. Preliminary version (1998) and Lindell, Yehuda, and Benny Pinkas. "Secure multiparty computation for privacy-preserving data mining." *Journal of Privacy and Confidentiality* 1.1 (2009): 5.

[29] Gentry, Craig. A fully homomorphic encryption scheme. Diss. Stanford University, 2009.

[30] F. Eigner, A. Kate, M. Maffei, F. Pampaloni, and I. Pryvalov, Achieving Optimal Utility for Distributed Differential Privacy Using Secure Multiparty Computation, in: P. Laud and L. Kamm (eds.), *Applications of Secure Multiparty Computation*, IOS Press, 2015, p. 82.

[31] Garfinkel, Simon. De-Identification of Personally Identifiable Information. Rep. no. 8053. N.p.: U.S. Department of Commerce NISTIR, April 2015. Print

[32] Sweeney, Latanya. "k-anonymity: A Model for Protecting Privacy." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05 (2002): 557–570 and Emam, Khaled El, and Fida Kamal Dankar. "Protecting Privacy Using K-Anonymity." *Journal of the American Medical Informatics Association: JAMIA. American Medical Informatics Association*, n.d. Web. November 11, 2015. And Machanavajjhala, Ashwin et al. "l-diversity: Privacy beyond k-anonymity." ACM Transactions on Knowledge Discovery from Data (TKDD) 1.1 (2007): 3. And Li, Ninghui, Tiancheng Li, and Suresh Venkatasubramanian. "t-closeness: Privacy beyond k-anonymity and l-diversity." Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on. IEEE, 2007.

(*Continued*)

Fig. 14.1 (continued)

[33] Tsymbal, Alexey et al. "The neighborhood graph for clinical case retrieval and decision support within health-e-child casereasoner." FGWM 09 (2009): 49. and

Gobeill, Julien et al. "Managing the data deluge: data-driven GO category assignment improves while complexity of functional annotation increases." Database 2013 (2013): bat041.

Müller, Henning, and HES SO. "Text-based (image) retrieval." (2010).

[34] Omiros Metaxas, Harry Dimitropoulos, Yannis Ioannidis, "AITION: A scalable KDD platform for Big Data Healthcare", in Proc. of the IEEE Int'l Conference on Biomedical & Health Informatics, Valencia, Spain, June 2014. <http://emb.citengine.com/event/bhi-2014/paper-details?pdID=177>

[35] Kahn, Robert E. "Overview of the Digital Object Architecture." *VLSI Electronics Microstructure Science VLSI and Computer Architecture* (1989): 165–95. CNRI. Web. March 28, 2016.

[36] Nakamoto, Satoshi. "Peer-to-Peer Directory System." *Legitimate Applications of Peer-to-Peer Networks* (2008): 109–22. Web. March 28, 2016. And "Ethereum Project." *Ethereum Project*. N.p., n.d. Web. March 28, 2016. And "What Is the Hyperledger Project?" Linux Foundation, n.d. Web. March 28, 2016.

[37] Watanabe, Hiroki et al. "Blockchain contract: A complete consensus using blockchain." *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)*. IEEE, 2015.

[38] Benitez, Kathleen, and Bradley Malin. "Evaluating re-identification risks with respect to the HIPAA privacy rule." *Journal of the American Medical Informatics Association* 17.2 (2010): 169–177.

[39] Wang, Linzhang, Eric Wong, and Dianxiang Xu. "A Threat Model Driven Approach for Security Testing." *Proceedings of the Third International Workshop on Software Engineering for Secure Systems*. IEEE Computer Society, 2007.

[40] Berlanga, Rafael et al. "Medical Data Integration and the Semantic Annotation of Medical Protocols." *Computer-Based Medical Systems, 2008. CBMS'08. 21st IEEE International Symposium on*. IEEE, 2008.

[41] Christen, Peter. *Data Matching: Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection*. Springer Science & Business Media, 2012.

[42] J. Kaye et al., Dynamic Consent, cit., p. 3.

The core of this foundational corpus can be found in the Universal Declaration of Human Rights, which protects an individual from "arbitrary interference with his privacy, family, home or correspondence" and "attacks upon his honour and reputation" (Article 12) (UN General Assembly 1948).

Additionally, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of

Personal Data (Council of Europe 1981) recognizes privacy (i.e., respecting an individual's "private and family life, his home and his correspondence" [Article 8]) as a fundamental human right. The European Charter of Fundamental Rights also defines the "respect for private and family life" (Article 7) and adds the "protection of personal data" (Article 8) (European Union 2000). These foundational texts, together with the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD 2002), constitute a solid "data protection corpus" on which the European directives noticeably build.

Rightly emphasized by the European Union, addressing privacy and regulatory obligations is not only a fundamental issue for the strengthening of individuals' trust in the digital world, it is also an essential element in the functioning of our democratic societies. In the USA, the Health Insurance Portability and Accountability Act (HIPAA 2016) has formalized a privacy rule. The European Commission did something similar with its Data Protection Directive (DPD) 95/46/EC (European Commission 1995) and E-Privacy Directive 2002/58/EC (EPD) (European Commission 2012).

More specifically, the DPD defines health data as a special category of data to which a higher level of data protection applies. Ali Gholami (Ali Gholami et al. 2014) identified a set of key principles from the DPD:

1. Lawfulness—all sensitive data processing must be conducted within the regulatory framework of the present directive
2. Informed consent (of the sample or data subject)—constitutes the main source of legitimacy for the processing of sensitive data
3. Purpose binding—ensures that personal data processing is performed according to predetermined purposes
4. Data minimization—restricts the extra or unnecessary disclosure of information to third parties, such as the platform itself in its role as the "processor"
5. Data accuracy—describes the necessity to keep data accurate and updated by the "controller"

6. Transparency—entitles the data subjects to have information about the processing of their data
7. Data security—proposes the implementation of technical measures to provide legitimate access and organizational safeguards
8. Accountability—mandates internal and external auditing, and control for various assurance reasons

Also important is that the DPD directive enables member states to reuse data for which consent to release had previously been received. According to Article 6(b), "further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible, provided that Member States provide appropriate safeguards" (European Union 1995). In medical research, safeguards usually consist of an assessment by an ethical review board, which may substitute for the consent of the subject after the risks and benefits of the proposed research have been assessed. Nevertheless, the DPD gives no clear definition about what "identifying information" actually is; thus, it left decades of space for the development of a plethora of privacy-enhancing technologies (Borking 2005) with different degrees of efficacy.

Twenty years later, the more binding GDPR (European Commission 2012) was finally promulgated in April 2016 at the European level. Over the next two years, it will become directly applicable to all member states and will not require national implementing legislation. Compared with the DPD and EPD, the GDPR, by setting out a number of ad hoc provisions, devotes more attention to the matter of health data and scientific research.

Generally speaking, such legislation emphasizes "privacy by design" and "privacy by default" approaches, thereby ensuring that confidentiality is at the very heart of the design, development, and maintenance of information systems. In other words, confidentiality is no longer considered a static and immutable property; rather, it becomes an evolving condition over time and with associated risks.

More importantly, the GDPR introduces new rights for the data subject to access, erase, or modify his/her data, or even to be digitally "forgotten" altogether, with administrative and legal sanctions applying if

these rights are violated. This important change was most certainly inspired by the world's first data protection law, the Data Protection Act Datenschutzgesetz [Data Protection Act] 1970, which was adopted by the State of Hesse, Germany, in October 1970.

Indeed, the most important factor in the subsequent development of privacy laws was the so-called census judgment by the German Federal Constitutional Court, which dealt with the question of informational self-determination. That judgment was based on the idea of *das allgemeine persönlichkeitsrecht* (general personality rights), which are enshrined in paragraph 2(1) of that country's constitution.

By recognizing the individual's natural rights over his/her personal data, the concept of informational self-determination makes a definitive step toward empowering the data subject (Rappaport 1981).

It is the author's belief that the combination of privacy by design, privacy by default, and the fundamental concept of informational self-determination establishes an unprecedented and powerful framework in Europe for the individual's empowerment in terms of the future collection of his/her data, and the processing of sensitive data. This framework has been further extended to the USA, thanks to the EU–US Privacy Shield adopted on July 12, 2016 (European Commission 2016a), thereby enabling Europeans to extend their rights across the Atlantic.

14.3 Digital Trust, Networks, and Technologies

Anticipating the complex needs of the GDPR regarding the protection of sensitive data and other privacy matters, a premiere network of hospitals and research centers was developed in the 2000s under the EU's Fifth Framework Programme's (FP5) MammoGrid project (Warren et al. 2007). Utilizing so-called grid computing (Foster et al. 2001), this network made it possible to share sensitive medical data across renowned European centers that were pioneering breast cancer

research. In doing so, some progress was achieved regarding the anonymizing of medical information (such as DICOM[2] file headers and images and diagnostic reports), as well as the secure sharing, indexing, cataloguing, and curating of data. This is what the outer layer of the privacy compass (Fig. 14.1) reports on.

The Health-e-Child[3] project builds on this idea and is even more ambitious in scope (Skaburskas et al. 2008). It focuses on the development of a distributed platform interconnecting several more centers and addressing three major pathologies in pediatrics.

This has resulted in an interesting strategy that allows for the sourcing and preparation of sensitive data from "the inside," with proper anonymization applied on site under the strict supervision of data managers. These managers have the power to manage quality and to quarantine or even stop the sharing of data at any time. The verified data is then uploaded to a demilitarized zone (isolated) server[4] storing federated (non-centralized) content from the other connected centers. By connecting to their routing systems (e.g., proprietary radiology information systems [RIS], pharmacy information systems [PIS], and picture archiving and communication systems [PACS] databases), this architecture also makes it possible to penetrate local information systems more deeply.

Today, a number of EU Seventh Framework Programme (FP7) projects further exploit and extend this initial network, with a total set of 15 centers feeding dedicated scientific data catalogues. These projects are:

- The Model-Driven European Paediatric Digital Repository (European Commission 2016b)

[2] Digital Imaging and Communications in Medicine (DICOM) is the standard for handling, storing, printing and transmitting medical imaging information.

[3] Health-e-Child is a European Commission project "aimed at developing a platform to integrate information from traditional and emerging sources to support personalized and preventative medicine as well as large-scale, data-based biomedical research and training" (see: http://cordis.europa.eu/project/rcn/105287_en.html).

[4] In computing, a demilitarized zone is a sub-network that separates an internal local area network (LAN) from other untrusted networks (such as the Internet).

- neuGRID, a web portal aimed at helping neuroscientists (Redolfi et al. 2009)
- N4U (neuGRID for you) (Frisoni et al. 2011)
- CARDIOPROOF (see: www.cardioproof.eu/about/overview-on-the-project)

Just as VISA developed a network of institutions accepting and supporting their credit cards, the intent of these projects is to further extend the initial network and keep feeding research platforms by providing access to more data. In the next three years, the author, in collaboration with concerned project partners, will therefore propagate this legacy network to give life to MyHealthMyData, which is a sustainable blockchain-enabled transactional platform. (A blockchain is a distributed database that maintains a growing list of records called blocks.) MyHealthMyData will serve to "top up" this privacy-preserving information system with full transparency and traceability over time and distance.

14.4 How a Blockchain Could Help

A blockchain is the technology behind Bitcoin (Nakamoto 2008). It is a cryptographic protocol that makes it possible to run a distributed, public, and trustable "ledger" where digital-object transactions are signed with the identities of the issuer and recipient, verified by a community of peers and stored as incremental blocks in a shared database. The major benefit of the blockchain is that it brings digital trust to a potentially untrustable network.

Now, think of this ledger enabling (anonymous) consents and data transactions deployed at a European scale. It would be browsable anytime, anywhere, and by anyone, yet contain no sensitive information. Imagine a place where individuals, research groups, pharmaceutical companies, and health-care professionals could easily search for and mobilize large volumes of data on demand, while ensuring clear patient consent and privacy at all times—regardless of data complexity, data-protection laws, or the patient's geographic location.

This is the author's objective: To create this type of solid technological backbone, supporting the resilience of information systems, and acting as an operational GDPR-compliant infrastructure where data transactions are informed and controlled by informational self-determination and privacy-by-design or privacy-by-default principles. Such a foundational base will open new avenues to innovative (smart) contracts (Watanabe et al. 2015) that incentivize data mobilization under strict regulatory control, while facilitating dynamic consent collection and data preparation.

Besides the advances the blockchain will bring to the development of a transparent, traceable, distributed, and trustable "ledger of consent" and its associated data transactions, it could also lead to experimentation with a novel type of social business model involving the use of specific protocols for exchanging value.

In effect, the result would be a new health-dedicated virtual currency that assigns economic value to different types of health-care transactions. Such state-of-the-art transitional money systems could "be used as crutches to re-educate atrophied collective behaviour patterns" (Lietaer 2001). The intent would be to investigate the potential use of shared economies and open-value accounting in health care (Bauwens et Stiegler 2015).

14.5 Conclusion

Although it is a fantastic opportunity to learn about ourselves, this wealth of suddenly accessible personal and sensitive data is a challenge for societies, which need to come up with advanced governance models that supplement their aggregate demand (AD) equation analyses with applicable ethical, legal, societal, and economical guidelines.

Comparable to the effect that Leonardo da Vinci's famous drawing of the Vitruvian Man had on our understanding of the proportions of a man's body (Vitruvius 1983), we are at the beginning of a new form of consciousness, a new source of knowledge that will provide humanity with an unprecedented chance to improve, learn, and grow.

However, right now, as individuals, we are "digitally naked," which is why we need to develop a digital skin—armor to protect us from outside attacks.

There is no doubt the Internet has greatly affected us all. Systemically enshrining the principles of privacy by design, privacy by default, and informational self-determination—using privacy-preserving technologies and the blockchain—may, in the longer term, better protect data subjects (i.e., you and me). And it may also direct society's information systems toward a fairer digital economy where "value" means more than money.

References

Borking, John, "The Use and Value of Privacy-Enhancing Technologies," *The Glass Consumer: Life in a Surveillance Society* (June 14, 2005): 69–96, doi:10.1332/policypress/9781861347350.003.0004.

Council of Europe "*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*," 108, Council of Europe, 1981.

Datenschutzgesetz [Data Protection Act] October 7, 1970, HESSISCHES GESETZ-UND VERORDNUNGSBLATT I.

European Commission "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)," COM (2012) 11 final, 2012/0011 (COD), Brussels, January 25, 2012.

European Commission "The EU-U.S. Privacy Shield," July 12, 2016a, accessed on October 3, 2016a, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

European Commission "Model-Driven European Paediatric Digital Repository," accessed October 3, 2016b, http://cordis.europa.eu/project/rcn/108228_en.html.

European Union "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Official, *Journal of the EC* 23, no. 6, (1995) European Parliament, Official Journal, OJ L 281 of (November 23, 1995).

European Union "Charter of Fundamental Rights of the European Union," (December 18, 2000), C 364/1 European Communities, Official Journal, 2000/C 364/01.

Foster, Ian, Carl Kesselman, and Steven Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," *International Journal of High Performance Computing Applications* 15, no. 3 (2001): 200–222, doi:/10.1109/ccgrid.2001.923162.

Frisoni, Giovanni B. et al., "Virtual Imaging Laboratories for Marker Discovery in Neurodegenerative Diseases," *Nature Reviews Neurology* 7, no. 8 (July 5, 2011): 429–438, doi:10.1038/nrneurol.2011.99.

Gholami, Ali et al., "Privacy Threat Modeling for Emerging BiobankClouds," *Procedia Computer Science* 37 (2014): 489–496, doi:10.1016/j.procs.2014.08.073.

Kish, Leonard J., and Eric J. Topol, "Unpatients—Why Patients Should Own Their Medical Data," *Nature Biotechnology* 33, no. 9 (September 8, 2015): 921–924, doi:10.1038/nbt.3340.

Lietaer, Bernard, "The Future of Money: Towards New Wealth, Work and a Wiser World," *European Business Review* 13, no. 2 (April 2001), doi:10.1108/ebr.2001.05413bab.008.

Michel Bauwens (with Jean Lievens), Sauver Le Monde. Vers Une économie Post-capitaliste Avec Le Peer-to-Peer, Paris, Éditions Les Liens qui libèrent, 2015, 268 p.

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, accessed on October 3, 2016, http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf.

OECD (2002), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publishing, doi: http://dx.doi.org/10.1787/9789264196391-en

Picard, Rosalind, and Gary Wolf, "Guest Editorial Sensor Informatics and Quantified Self," *IEEE Journal of Biomedical and Health Informatics* 19, no. 5 (September, 2015): 1531–1531, doi:10.1109/JBHI.2015.2462372.

Rappaport, Julian, "In Praise of Paradox: A Social Policy of Empowerment over Prevention," *American Journal of Community Psychology* 9, no. 1 (1981): 1–25.

Redolfi, Alberto et al., "Grid Infrastructures for Computational Neuroscience: The neuGRID example," *Future Neurology* 4, no. 6 (2009): 703–722.

Skaburskas, Konstantin et al., "Health-e-Child: A Grid Platform for European Paediatrics," *Journal of Physics: Conference Series* 119, no. 8, 082011 (IOP Publishing, 2008), doi:10.1088/1742-6596/119/8/082011.

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), accessed on February 24, 2017, http://www.refworld.org/docid/3ae6b3712c.html

United States "*Health Insurance Portability and Accountability Act (HIPAA)*," Washington, DC, U.S: Dept. of Labor, accessed on October 3, 2016, http://purl.fdlp.gov/GPO/gpo10291.

Vitruvius, Marcus Pollio, "De architectura," 2 volumes, translated by F. Granger, Loeb Classical Library," (1983).

Warren, R. et al., "MammoGrid—A Prototype Distributed Mammographic Database for Europe," *Clinical Radiology* 62, no. 11 (November 2007): 1044–1051, doi:10.1016/j.crad.2006.09.032.

Watanabe, Hiroki et al., "Blockchain Contract: A Complete Consensus Using Blockchain," *In 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)* (October 2015): 577–578, doi:10.1109/gcce.2015.7398721.