Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

Governance of artificial intelligence and personal health information

Jenifer Sunrise Winter and Elizabeth Davidson

University of Hawaii at Manoa

Citation – Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

Abstract

Purpose – This paper aims to assess the increasing challenges to governing the personal health information (PHI) essential for advancing artificial intelligence (AI) machine learning innovations in health care. Risks to privacy and justice/equity are discussed, along with potential solutions.

Design/methodology/approach – This conceptual paper highlights the scale and scope of PHI data consumed by deep learning algorithms and their opacity as novel challenges to health data governance. Findings – This paper argues that these characteristics of machine learning will overwhelm existing data governance approaches such as privacy regulation and informed consent. Enhanced governance techniques and tools will be required to help preserve the autonomy and rights of individuals to control their PHI. Debate among all stakeholders and informed critique of how, and for whom, PHI-fueled health AI are developed and deployed are needed to channel these innovations in societally beneficial directions. Social implications – Health data may be used to address pressing societal concerns, such as operational and system-level improvement, and innovations such as personalized medicine. This paper informs work seeking to harness these resources for societal good amidst many competing value claims and substantial risks for privacy and security.

Originality/value – This is the first paper focusing on health data governance in relation to AI/machine learning.

Keywords – Big data, Governance, Artificial intelligence, Deep learning, Personal health information

1. Introduction and motivation

Artificial intelligence (AI) technologies increasingly enable innovations from searching the internet to voice and facial recognition, smart appliances, and even to driverless cars. In the past, key limitations of AI have been the availability of sufficient data for training algorithms and the inability of AI systems to manage data in their natural form. Now, with omnipresent

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

digitalization of data about humans and their activities, deep learning[1] algorithms increasingly are able to take advantage of stockpiles of "big data" to enhance a learning model's performance and extend the sophistication and reach of AI applications (Chen and Lin, 2014; Jordan and Mitchell, 2015).

AI innovations are particularly promising in the domain of health and health-care services. From personalized health care tailored for each individual's biology to improvements in health-care delivery systems, AI innovations are projected to revolutionize health-care outcomes for individuals and for health-care systems (Flores et al., 2013). Vital to these potential innovations are the vast stockpiles of individual-level health data needed for deep learning models. Now, personal health information (PHI)[2] data stores, such as notes from routine visits to the doctor, medical imaging, self-monitoring of steps, sleep and heartbeats, and DNA repositories, are rapidly accumulating, and will over time (given much-needed improvements in data quality and standardization), be applied to train deep learning algorithms in the growing array of AI health-care applications (Miotto et al., 2017).

The combination of AI, deep learning and digitized PHI data has been heralded as transformational for health care (Siwicki, 2017; Sullivan, 2017). Recognizing the potential of highly profitable health-care markets, information technology (IT) giants such as Alphabet/ Google, Microsoft, Apple, and IBM, along with dozens of technology startups, are partnering with health-care systems and investing in health-related mobile devices, health- care applications and AI technologies. In Europe and the USA alone, health-care AI markets have been valued in the hundreds of millions of Euros and are forecast to grow to over e7bn in Europe and e14bn in the USA by 2027 (PRNewswire, 2018).

Compared to the projected benefits from health-care AI, much less consideration has yet been given to possible unintended or undesirable consequences of these developments for individuals and for society. Many questions remain unanswered and will grow in importance. For instance, who will pay the costs and who will reap the benefits of health- related AI innovations? Will costly advances in personalized medicine be limited to wealthy nations (as was seen with AIDS drugs), or even to the wealthy few in these nations? Will PHI be linked to innocuous trace activity data through AI/machine learning methods and used to limit an individual's access to social and economic opportunities, based on that individual's predicted health status? How can we best govern algorithms to reduce risk amidst complex systems with a high degree of uncertainty? (Saurwein et al., 2015). These are just a few of the ethical and societal issues than need to be surfaced and debated as governments, health systems, and importantly, global IT firms aggressively pursue AI ventures in health care.

In this paper, we draw on Giddens's metaphor of the relentless scientific progress of modernity as a juggernaut – a powerful and dangerous force that is difficult to steer (Giddens, 1990, p. 151) – to focus attention on one critical aspect of what may be a developing health-care AI juggernaut: the challenges of governing the PHI data that are essential to advancing AI and

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

machine learning in health care. PHI data governance addresses privacy, security, ownership and use and reuse of health data as well as the underlying values and interests that shape data governance structures (Winter and Davidson, 2017). We highlight two attributes of AI deep learning that, while not unique to the health-care setting, pose significant and novel challenges to PHI data governance: the scale and scope of data consumed by deep learning algorithms, and the opacity of algorithms in regards to how data are utilized and new data or results are produced. We then argue that existing data governance structures will not be sufficient to address the radical uses and reuse of PHI data brought about by deep learning technologies, focusing on two common governance approaches: preemptive privacy regulation and informed consent. We conclude by considering new approaches to data governance required to enable accessibility of PHI for AI innovations but also to preserve the autonomy and rights of individuals to control their PHI and to channel the power of AI and machine learning for health-care transformation in societally beneficial directions.

1.1 Fueling the artificial intelligence health-care juggernaut

PHI data governance is concerned with balancing individual privacy, authorized access to PHI data, and data security with the benefits of utilizing data for health system improvement and innovation (Hripcsak et al., 2014; Rosenbaum, 2010). Government regulators and researchers have advocated for health data sharing and for standards and infrastructures to enable health data interoperability (Blumenthal, 2010; Hripcsak et al., 2014; Rosenbaum, 2010). A tacit assumption is that wide-scale sharing of health data will necessarily serve the public good. Given the economic value that may be exploited from PHI data to serve corporate interests, such assumptions are not fully warranted (Harper, 2013; Rosenbaum, 2010). Now, with AI and machine learning at the frontier of health system transformation, novel, and heightened, challenges to PHI data governance must be addressed.

2. The complexity of personal health information data and challenges of data governance

The term PHI data relates to a variety of data domains that contain personally identifying (or potentially identifying) characteristics: medical history data; clinical data collected in EHR systems of hospitals, physicians, and laboratories; pharmacy prescription data; patient- generated health data from medical devices (such as a glucose monitor) or general purpose activity tracker (such as a Fitbit step tracking device); and medical expense claims data. Other PHI data domains are created by analyzing data not directly connected to health status, but health status can be inferred analytically. These data can be characterized as consumer-generated health data, for instance trace data from internet search activities, credit card purchases and online shopping, or geospatial/location data.

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

These various PHI data are governed by an equally wide variety of stakeholders from health-care providers to retailers to IT firms. Data governance has been defined as "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods" (Data Governance Institute, n.d., para. 2). In the information systems field, data governance refers primarily to management of organizational data by that organization (Khatri and Brown, 2010), but new forms of inter-organizational data governance are also developing to take advantage of "big data" and advancing analytics capabilities such as AI, for instance data collaboratives in fields such as genetics research and clinical trials (Perkmann and Schildt, 2015; Susha et al., 2017) and distributed research networks (DRNs) (Holmes et al., 2014).

Effective health data governance remains an elusive goal for myriad reasons, and with ever increasing digital stockpiles of digitized PHI, a growing challenge (Hripcsak, 2014; Rosenbaum, 2010). First, digitized health data are created in health IT (HIT) systems spread across a variety of collaborative and competing organizations, including hospitals, physician practices, nursing homes, third-party payers (insurers) including state and federal governments, pharmacies, testing laboratories, and increasingly, by IT vendors that provide HIT systems. This results in the lack of data standardization and interoperability that currently presents substantive barriers to PHI data sharing and data use, including use in advanced analytics and AI applications. Second, regulations intended to limit the disclosure of personally-identifiable health data (such as HIPAA in the USA or GDPR in the European Union) have limited the flow and increased costs to researchers to access PHI data for societally sanctioned purposes (Lane and Schur, 2010). Third, with rising popularity of health monitoring devices and applications, patient-generated health data (PGHD) resources are developing outside of clinical settings and health data regulatory oversight (Deering et al., 2013). Individuals create PHI through wearable activity monitors or share their PHI with commercial firms (e.g. for genetic profiling) or patient support groups (Tempini, 2017). In many instances, these data are not covered by health privacy protection legislation as consumers, often unwittingly, grant to the commercial firm (e.g. Fitbit, Apple, 23andMe) governance rights for these data.

There are substantive challenges for governing PHI data so as to balance the varied interests of diverse stakeholders – individuals, health-care practitioners, regulators, third- party health-care funders, health-care innovators including IT firms, and so on. Despite existing issues, there are nonetheless relentless societal and regulatory pressures to make PHI data even more available for research and innovation (Siwicki, 2017; Sullivan, 2017) so as to realize the transformations in health and health services projected from these developments. The possibilities of AI and deep learning both increase these pressures and create even more challenges for PHI data governance. Next, we highlight two such challenges: the scale and scope of PHI utilized by these advances and the opacity of the AI algorithms.

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

2.1 Scale and scope of personal health information data aggregation and use

Deep learning algorithms rely on massive data sets to train and improve AI models (Chen and Lin, 2014; Jordan and Mitchell, 2015). The growing stockpiles of digitized PHI data available through research and commercial arrangements provide essential fuel for deep learning innovation in health care (Murdoch and Detsky, 2013). PHI data include a broad array of data from routine transactions to novel data types such as Internet-of-Things medical devices embedded in clinical settings, daily life and even in human bodies (Deering et al., 2013). In many countries, data on health services encounters (e.g. doctor visits, hospital care) are captured in electronic health record systems. Transactions such as filling a prescription or purchasing an over-the-counter medication are digitally recorded (e.g. by retail pharmacies). Search engines such as Google capture individuals' search histories for health-related information, while social media platforms collect and correlate data on health-related interactions (Eichler et al., 2016; Sarasohn-Kahn, 2014). Although these PHI data are scattered across data platforms today, in the future, as deep learning algorithms become more sophisticated, these various data sources are likely to be compiled, linked, made available for reuse (possibly sold between private brokers) and then used to develop profiles of individuals' behaviors and for predictive health models (Bates et al., 2014; Cohen et al., 2014; Siegel, 2016).

That is, the scale and scope of personally identifiable health-related data that will be available in the near future for AI and deep learning have increased dramatically in the last decade. Moreover, trace data that are not specifically related to health are also collected and mined to link everyday activities (Web browsing, household activities harvested through devices such as Alexa or Google Home, television viewing habits, supermarket purchases) to health status or behaviors (Mai, 2016). These trace data, which are not protected by health data privacy regulations or even acknowledged explicitly as health- related, "can be combined with personal information from other sources–including health- care providers and drug companies–raising such potential harms as discriminatory profiling, manipulative marketing, and data breaches" (Montgomery et al., 2018, p. 42).

Deep learning algorithms also create a whole new category of predictive health data about individual and group behaviors. As Kitchin and Lauriault (2016, p. 12) note, "a person's data shadow does more than follow them; it precedes them" when used for predictive profiling and social sorting into categories. For instance, behavioral data from web searches or biometric data from fitness trackers can be linked to other data sources to create profiles of individuals. These models of probabilities, as well as a wide variety of metadata and trace data about daily activities, can be used to categorize individuals, make predictions about their behavior, and then to prioritize the use of health-care resources based on these profiles (Cohen et al., 2014), without the profiled individual's consent or awareness.

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

2.2 Opacity of personal health information data in artificial intelligence algorithms

A lack of transparency in corporate-public data sharing arrangements in AI partnerships, and the inherent opacity of deep learning algorithms raise questions about the feasibility of effective PHI data governance. For instance, Xiao et al. (2018), note that "to bring deep models built from EHR [electronic health records] data into real use, users often need to understand the mechanisms by which models operate. Such a level of model transparency is still challenging to achieve" (p. 1425). Deep learning is a "black box" (Pasquale, 2015), with its inner workings obscured by the opacity and complexity of algorithms. Despite efforts towards interpretable machine learning and AI, and "explainable AI", which use mathematics to simplify black boxes, human understanding and real-world application of these abstractions is still problematic (Abdul et al., 2017). Burrell (2016) observes that this opacity is at the center of growing concerns about algorithms by legal scholars and social scientists. In some cases, opacity may be an "intentional corporate or institutional self-protection and concealment" (Burrell, 2016, pp. 1-2), particularly to protect corporate intellectual property and competitive advantage. In others, those examining an AI system may lack the specialized coding skills to understand its processes. A third type of opacity, characteristic of deep learning, relates to the scale and complexity of machine learning, and thus to humans' difficulty understanding an algorithm in action as it reads real-time data and adapts. Burrell (2016, p. 5) comments, "Though a machine learning algorithm can be implemented simply in such a way that its logic is almost fully comprehensible, in practice, such an instance is unlikely to be particularly useful".

Thus, increasingly, opacity is inherent in the process of developing and deploying AI deep learning algorithms across many data domains and applications (Faraj et al., 2018). In the health-care domain, opacity is problematic not only for monitoring what PHI data are used, but also for understanding the purposes and outcomes of data use, for instance the possibility of discriminatory profiling. Barocas and Selbst (2016) argue that discrimination is often an "unintentional emergent property of the algorithm's use rather than a conscious choice by its programmers, [but] it can be unusually hard to identify the source of the problem or to explain it to a court" (Barocas and Selbst, 2016, p. 1). Burrell's latter category (human ability to understand the algorithm's operation) makes specifying and monitoring PHI data governance particularly problematic.

3. Controlling the health-care artificial intelligence juggernaut

Given the sensitivity of personal health data and existing legal and regulatory protections, PHI data governance approaches are more mature than in many socioeconomic sectors (Hripcsak et

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

al., 2014; Rosenbaum, 2010). However, existing PHI data governance structures are unlikely to be sufficient to control the combined momentum of AI, deep learning and aggregation of PHI, or thus to help channel developments along societally beneficial and equitable directions.

3.1 Preemptive health data regulation

Data protections vary from country to country, but even the most stringent regulations may prove to be ineffective to manage the flow of PHI data into AI ventures and thus into the purview of varied public, private, and for-profit stakeholders. Effective regulation depends on clear and comprehensive articulation of regulatory requirements as well as the regulating authority's ability to evaluate and monitor compliance (Jordan and Mitchell, 2015). Good- faith compliance with regulations is also important, as the harm resulting from violations may be difficult to detect and to repair.

The European Union is focusing on digitization of health care, fostering standardization of electronic health records and developing data analytics and AI to enhance innovation and improve care (European Commission, 2018). The recent European Union General Data Protection Regulation (GDPR, European Parliament and Council of the European Union, 2017) grants individuals multiple rights (e.g. the "Non-Discrimination Right", the "Right to Explanation", and the "Right to Be Forgotten"), and health data are afforded a special category requiring higher protection. The GDPR is currently the strongest data protection regime in the world; however, it may be inadequate to address the tradeoffs between individual privacy and autonomy and the promised individual, societal and economic benefits of health-care AI ventures. For example, the scale and scope of PHI data necessary for training deep learning algorithms, and the opacity of how these algorithms operate, make accurate and comprehensive articulation of data use regulations and the monitoring of compliance with PHI data regulations very difficult (Kuner et al., 2017). For instance, Article 22(1) of the GDPR relates to "personal data used for automated decisions" and specifies that data should only be gathered for "specified, explicit, and legitimate purposes, and subsequent processing that is incompatible with those purposes is not permitted" (Kuner et al., 2017, p. 3). However, as large amounts of PHI data must be processed to train deep learning models (Xiao et al., 2018), developing these models will likely rely on the reuse of a variety of PHI data that are collected for other purposes (such as providing a health-care service or payment for services).

Is a deep learning model developed to predict disease progression and health-care resource consumption compatible with those purposes? Because of the scale and scope of PHI data needed to effectively train models and the dynamic nature of data use in deep learning, "it may be difficult to reconcile such dynamic processes with purposes that are specified narrowly in advance" (Kuner et al., 2017, p. 3). The opacity of algorithmic processes and the conclusions generated, such as predictive profiles, make monitoring compliance difficult and may also mask

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

potential harm from regulatory oversight, particularly in areas not directly related to health care (e.g. health-related discrimination in employment or access to financial services like credit or insurance).

The temptation for organizations that control PHI to interpret broadly, or even disregard, PHI data regulations in the face of the much-heralded potential of AI innovation was evident in a recent case in the UK Despite the UK's stringent health data privacy laws, in 2015, a National Health Services (NHS) hospital system (Royal Free) provided five years of medical data on 1.6 million of its patients to a commercial, for-profit AI venture (Alphabet DeepMind Health). Data were provided in an open-ended agreement intended to help DeepMind develop health-care AI applications that Royal Free patients might later benefit from (Hawkes, 2016). In 2017, the UK Information Commissioner's Office (ICO) ruled that the DMH-Royal Free data sharing agreement had not complied with existing data protection laws. In response to regulatory concerns, Royal Free and DeepMind Health subsequently enhanced their self-regulation PHI governance procedures, but they also extended their data sharing agreement for another five years (Lomas, 2017), an indication of the strong lure of AI innovation for health service providers and IT firms.

3.2 Informed consent

As deep learning broadens the scope and scale of data used in health-care analytics, the concept of informed consent is itself challenged. For instance, a patient may authorize sharing of her health data to facilitate delivery of health-care services (to herself) and of payments from third-party payers. Her PHI then falls under the control of various organizations, which may later share her data for health research or use in system-wide efficiency analytics, and even for sale (within regulatory limitations). The promises of health system transformation through AI and machine learning increase the appeal of such data sharing arrangements, as was seen in the NHS Royal Free-DeepMind Health case. Royal Free administrators claimed that explicit patient consent for data sharing was not required and could be assumed, because (some of the) PHI data were to be used for direct care of (some) patients (Hawkes, 2016).

A regulatory workaround to grant access to PHI data without an individual's informed consent is to de-identify patient data. However, (re)identified data are more valuable for AI deep learning to recognize and exploit associations among data sources. Re-identification of PHI data subverts regulatory intent but it is not difficult technically (El Emam et al., 2011; Rothstein, 2010). For example, Facebook founder Mark Zuckerberg revealed in testimony before the US Congress in April 2018 that his company collects some health data about individuals. That same month, it was revealed that Facebook had initiated a project to gain anonymized patient data to "match hospitals' patient data on diagnoses and prescription information with Facebook so the company could combine that data with its own to construct digital profiles of patients [.. .] Facebook's

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

stated intent was never to leave the data anonymized. But requesting the hospitals' data in that form would allow Facebook to sidestep the issue of obtaining patients' consent, as required by federal law" (Ostherr, 2018, para. 5-6). This instance illustrates the economic value that commercial firms operating outside of the health-care setting, here a social media firm, are looking to harvest from PHI through advanced analytics and AI. This instance also illustrates how one's data shadow from a variety of daily activities (e.g. Facebook postings) can be merged with ostensibly protected health data outside the boundaries of informed consent practices.

Genomic data and their use in precision genomics provide another illustration of the limits of informed consent arising from the networked properties of PHI data. One individual's DNA is part of a biological (and now informational) network that extends to ancestors, family members and relatives, and future descendants (Azencott, 2018). Speaking broadly of data privacy, boyd (2012) describes this as networked privacy: "What we share about ourselves tells heaps about other people" (boyd, 2012, p. 1). Precision genomics rely on a variety of data-intensive tests to understand variants in DNA sequences and their health implications, and thus on widespread sharing of a broad, varied scope of PHI including DNA (Aronson and Rehm, 2015). While medical records tend to focus on individual patients who may consent to the use of this data, one individual's DNA may reveal sensitive personal information about others who have not consented to share it (or have even been born). Groups such as the Regulatory and Ethics Working Group of the Global Alliance for Genomics and Health have created frameworks for the responsible sharing of genomic data, as well as standards for obtaining consent. However, as with other forms of PHI, these "DNA networks" housed across multiple genomics repositories are also susceptible to (re) identification (Gymrek et al., 2013).

3.3 Enhancing personal health information data governance structures

We have argued that preemptive data use regulations will not be sufficient to address the scale and scope of PHI data utilization and the opacity of AI deep learning algorithms. Beyond governing the inputs of deep learning, heightened governance of the processes and uses (outputs) of deep learning will also be needed. For instance, in response to growing concerns about data ethics and negative social consequences, interdisciplinary scholars have begun to develop field experiments that detect discrimination arising from AI and big data analytics (Sandvig et al., 2014). Ironically, deep learning methods can be applied to detect unintended or intentional societal effects from deep learning. This approach is echoed by the Royal Statistical Society's (Royal Statistical Society, 2016) call for an inquiry about "methods that the public can use to hold algorithms to account" (Royal Statistical Society, 2016, p. 3). These "algorithmic audits" will initially be limited because of the opacity of AI algorithms and laws that protect proprietary systems and intellectual property. However, there is some promise in requiring auditability to be designed into systems so that that AI and deep learning systems create an audit trail explaining what data were accessed and how data were used. For example, Alphabet's DeepMind Health AI

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

venture has designed a technical governance structure, the "Verifiable Data Audit", which uses a technology similar to blockchain to provide a real-time audit and verification of PHI data access and use (DeepMind, 2017). DeepMind intends that this will make its use of PHI data more transparent to authorized reviewers. In this case, the novel technique is intended to govern the process of data analysis and predictive modeling.

As current informed consent practices will not suffice to govern the scale and scope of PHI data utilized in AI deep learning ventures, more advanced sociotechnical solutions will be needed. Sharon (2016) argues that much research using big data sets challenges traditional understanding of informed consent because related risks cannot be forecast at the time of collection; thus, new models of open, broad and portable consent are being developed for research purposes. Beyond the ethical questions of using PHI in research is "the unavoidable question of who stands to benefit and in which way from research results" (Sharon, 2016, p. 568). Because AI algorithms themselves still belong to some human entity, the outputs and uses of outputs of deep learning methods could also become subject to regulation. Requirements might be voluntary in some cases and in others may require multilayered regulation to ensure compliance. Articulating such regulations will require personnel with sufficient training in deep learning methods to understand their consequences, as well as public debate about the compromises that allowing, or restricting, such innovations may entail (Singer, 2018).

4. Concluding remarks

Giddens (1990) termed circumstances in which the momentum to pursue scientific advancements crushes consideration of possible societal consequences as a juggernaut. In this essay, we have questioned whether growing trends towards (relatively) unfettered use of personal health data in machine learning will fuel a health AI juggernaut. The promises of health, health services, and health system transformation that might be possible through AI/ machine learning innovations are substantial and compelling. We argued that the scale and scope of PHI data consumed by deep learning models and the opacity of these algorithms will overwhelm current approaches to PHI data governance, in particular, preemptive data regulations and informed consent practices. To merely maintain some balance between individual rights and autonomy, and corporate interests in extracting value from PHI through AI, new data governance techniques and tools will be required.

To mitigate high-consequence risks of the juggernaut, Giddens advocates for us to "envision alternative futures whose very propagation might help them be realized" (1990, p. 154). IS scholarship can inform, and thereby help actualize, more desirable futures by illuminating the diverse interests, values, and conflicts underlying technology developments (Chiasson et al., 2018). As a small contribution to this larger program, our focus here has been on the aggregation, use, and reuse of PHI and other data for AI deep learning and the challenges to data

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

governance these innovations pose. Enhancing PHI data governance approaches is critically important, but this alone this will not control the health AI juggernaut. Questions of who benefits from, and who pays the price for, health AI developments remain. We will need to look beyond the glowing promises and allure of health and health-care systems "transformed" by AI to consider which stakeholder interests and values are (or will) be served by various AI ventures, and to debate whose interests and values should be served. As one example, intentional opacity of data sharing agreements and learning model operations that limit effective PHI data governance can lead to debates on whether health AI ventures should be governed by intellectual property rights of corporations or conducted within the public domain for the public good. Reasoned critique is required, as well as empirical study of developments and their consequences, to help ensure health AI will contribute to the broader public interest as well as to individual well-being in the future.

Notes

1. Machine learning, a subset of artificial intelligence, enables many functions of modern industrial societies – from searching the Web, voice and facial recognition, smart appliances, to driverless cars. A key limitation of traditional machine learning has been its inability to manage data in their natural form, requiring transformation of raw data into meaningful features (i.e. individual, measurable characteristics). Deep learning is a subset of machine learning that relies on massive amounts of raw data to enhance model performance. Deep learning is already widely applied across a range of domains, including healthcare.

2. In the United States context, PHI refers to Protected Health Information or Personal Health Information. We broadly use the term PHI to refer to "personal health data".

References

Abdul, A., Vermeulen, J., Wang, D., Lim, B.Y. and Kankanhalli, M. (2017), "Trends and trajectories for explainable, accountable, and intelligible systems: an HCI research agenda", CHI 2018, April 21-26, Montreal.

Aronson, S.J. and Rehm, H.L. (2015), "Building the foundation for genomics in precision medicine",

Nature, Vol. 526 No. 7573, pp. 336-342.

Azencott, C.-A. (2018), "Machine learning and genomics: precision medicine vs patient privacy", arXiv:1802.10568v2 [cs.CY].

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

Barocas, S. and Selbst, A.D. (2016), "Big data's disparate impact", California Law Review, Vol. 104 No. 3, pp. 671-732.

Bates, D.W., Saria, S., Ohno-Machado, L., Shah, A. and Escobar, G. (2014), "Big data in health care: using analytics to identify and manage high-risk and high-cost patients", Health Affairs , Vol. 33 No. 7, pp. 1123-1131.

Blumenthal, D. (2010), "Launching HITECH", New England Journal of Medicine, Vol. 62, pp. 382-385. boyd, d. (2012), "Networked privacy", Surveillance & Society, Vol. 10 Nos 3/4, pp. 348-350.

Burrell, J. (2016), "How the machine 'thinks': understanding opacity in machine learning algorithms", Big Data & Society, available at: https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512

Chen, X.W. and Lin, X. (2014), "Big data deep learning: challenges and perspectives", IEEE Access, Vol. 2, pp. 514-525.

Chiasson, M., Davidson, E. and Winter, J. (2018), "Philosophical foundations for informing the future(S) through IS research special issue on IS and philosophy", European Journal of Information Systems, Vol. 27 No. 3, pp. 367-379, doi: 10.1080/0960085X.2018.1435232.

Cohen, I.G., Amarasingham, R., Shah, A., Xie, B. and Lo, B. (2014), "The legal and ethical concerns that arise from using complex predictive analytics in health care", Health Affairs, Vol. 33 No. 7, pp. 1139-1147.

Data Governance Institute (n.d.), "Data governance definition", available at: www.datagovernance.com/ adg_data_governance_definition/ (accessed 11 November 2017).

DeepMind (2017), "Trust, confidence and verifiable data audit", available at: https://deepmind.com/blog/ trust-confidence-verifiable-data-audit/ (accessed 20 November 2017).

Deering, M.J., Siminerio, E. and Weinstein, S. (2013), "Patient-generated health data and health IT", Office of the National Coordinator for Health Information Technology, pp. 1-11.

Eichler, G.S., Cochin, E., Han, J., Hu, S., Vaughan, T.E., Wicks, P., Barr, C. and Devenport, J. (2016), "Exploring concordance of patient-reported information on PatientsLikeMe and medical claims data at the patient level", Journal of Medical Internet Research, Vol. 18 No. 5, doi: 10.2196/jmir.5130.

El Emam, K., Jonker, E., Arbuckle, L. and Malin, B. (2011), "A systematic review of re-identification attacks on health data", PloS One, Vol. 6 No. 12, p. e28071.

European Commission (2018), "Enabling the digital transformation of health and care in the digital single market; empowering citizens and building a healthier society", SWD(2018) 126 final, available at: http:// ec.europa.eu/newsroom/dae/document.cfm?doc_id=51628

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

European Parliament and Council of the European Union (2017), "General data protection regulation", available at: https://gdpr-info.eu/

Faraj, S., Pachidi, S. and Sayegh, K. (2018), "Working and organizing in the age of the learning algorithm", Information and Organization, Vol. 28 No. 1, pp. 62-70.

Flores, M., Glusman, G., Brogaard, K., Price, N.D. and Hood, L. (2013), "P4 medicine: how systems medicine will transform the healthcare sector and society", Personal Medicine, Vol. 2013 No. 10, pp. 565-576.

Giddens, A. (1990), The Consequences of Modernity, Stanford University Press, Stanford.

Gymrek, M., McGuire, A.L., Golan, D., Halperin, E. and Erlich, Y. (2013), "Identifying personal genomes by surname inference", Science, Vol. 339 No. 6117, pp. 321-324.

Harper, E.M. (2013), "The economic value of health care data", Nursing Administration Quarterly, Vol. 37 No. 2, pp. 105-108.

Hawkes, N. (2016), "NHS data sharing deal with Google prompts concern", The British Medical Journal, Vol. 353 No. 2573.

Holmes, J.H., Elliott, T.E., Brown, J.S., Raebel, M.A., Davidson, A., Nelson, A.F. and Steiner, J.F. (2014), "Clinical research data warehouse governance for distributed research networks in the USA: a systematic review of the literature", Journal of the American Medical Informatics Association, Vol. 21 No. 4, pp. 730-736.

Hripcsak, G., Bloomrosen, M., FlatelyBrennan, P., Chute, C.G., Cimino, J., Detmer, D.E., Edmunds, M., Embi, P.J., Goldstein, M.M., Hammond, W.E., Keenan, G.M., Labkoff, S., Murphy, S., Safran, C., Speedie, S., Strasberg, H., Temple, F. and Wilcox, A.B. (2014), "Health data use, stewardship, and governance: ongoing gaps and challenges: a report from AMIA's 2012 health policy meeting", Journal of the American Medical Informatics Association : JAMIA, Vol. 21 No. 2, pp. 204-211.

Jordan, M.I. and Mitchell, T.M. (2015), "Machine learning: trends, perspectives, and prospects", Science, Vol. 349 No. 6245, pp. 255-260.

Khatri, V. and Brown, C.V. (2010), "Designing data governance", Communications of the ACM, Vol. 53 No. 1, pp. 148-152.

Kitchin, R. and Lauriault, T.P. (2016), "Towards critical data studies: charting and unpacking data assemblages and their work", available at: www.nuim.ie/progcity/ (accessed 24 January 2018).

Kuner, C., Svantesson, D.J.B., Cate, F.H., Lynskey, O. and Millard, C. (2017), "Machine learning with personal data: is data protection law smart enough to meet the challenge?", International Data Privacy Law, Vol. 7 No. 1, pp. 1-2.

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

Lane, J. and Schur, C. (2010), "Balancing access to health data and privacy: a review of the issues and approaches for the future", Health Services Research, Vol. 45 No. 5 Pt 2, pp. 1456-1467.

Lomas, N. (2017), "DeepMind health inks another 5-year NHS app deal in face of ongoing controversy", TechCrunch, available at: https://techcrunch.com/2017/06/22/deepmind-health-inks-another-5-year- nhs-app-deal-in-face-of-ongoing-controversy/ (accessed 7 December 2017).

Mai, J.E. (2016), "Big data privacy: the datafication of personal information", The Information Society, Vol. 32 No. 3, pp. 192-199.

Miotto, R. Wang, F. Wang, S. Jiang, X. and Dudley, J.T. (2017), "Deep learning for healthcare: review, opportunities and challenges", Briefings in Bioinformatics, available at: https://academic.oup.com/bib/ advance-article-abstract/doi/10.1093/bib/bbx044/3800524? (accessed 25 May 2018).

Montgomery, K., Chester, J. and Kopp, K. (2018), "Health wearables: ensuring fairness, preventing discrimination, and promoting equity in an emerging internet-of-Things environment", Journal of Information Policy, Vol. No. 8, pp. 34-77.

Murdoch, T.B. and Detsky, A.S. (2013), "The inevitable application of big data to health care", JAMA, Vol. 309 No. 13, pp. 1351-1352.

Ostherr, K. (2018), "Facebook knows a ton about your health. Now they want to make money off it", available at: www.washingtonpost.com/news/posteverything/wp/2018/04/18/facebook-knows-a-ton-about- your-health-now-they-want-to-make-money-off-it/? (accessed 5 May 2018).

Pasquale, F. (2015), The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, Cambridge, MA.

Perkmann, M. and Schildt, H. (2015), "Open data partnerships between firms and universities: the role of boundary organizations", Research Policy, Vol. 44 No. 5, pp. 1133-1143.

PRNewswire (2018), "Global AI in healthcare market report for 2016-2027", available at: www.prnewswire. com/news-releases/global-ai-in-healthcare-market-report-for-2016-2027-300576951.html (accessed 12 April 2018).

Rosenbaum, S. (2010), "Data governance and stewardship: designing data stewardship entities and advancing data access", Health Services Research, Vol. 45 No. 5p2, pp. 1442-1455.

Rothstein, M.A. (2010), "Is deidentification sufficient to protect health privacy in research?", The American Journal of Bioethics, Vol. 10 No. 9, pp. 3-11.

Royal Statistical Society (2016), "Evidence to the royal society and British academy on data governance", available at: www.rss.org.uk/Images/PDF/influencingchange/2016/RSS-

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

evidence-to-Royal-Society-and- British-Academy-on-DataGovernance-Nov-2016.pdf (accessed 3 April 2018).

Sandvig, C., Hamilton, K., Karahalios, K. and Langbort, C. (2014), "Auditing algorithms: research methods for detecting discrimination on internet platforms", Data and Discrimination: Converting Critical Concerns into Productive Inquiry, International Communication Association Annual Conference, Seattle, WA.

Sarasohn-Kahn, J. (2014), "Here's looking at you: how personal health information is being tracked and used", California Healthcare Foundation, available at: https://goo.gl/YCaEFM (accessed 24 November 2017).

Saurwein, F., Just, N. and Latzer, M. (2015), "Governance of algorithms: options and limitations", info, Vol. 17 No. 6, pp. 35-49, available at: https://doi.org/10.1108/info-05-2015-0025

Sharon, T. (2016), "The googlization of health research: from disruptive innovation to disruptive ethics", Personalized Medicine, Vol. 13 No. 6, pp. 563-574.

Siegel, E. (2016), Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, John Wiley & Sons, Hoboken, NJ.

Singer, N. (2018), What you don't know about how Facebook uses your data, available at: www.nytimes. com/2018/04/11/technology/facebook-privacy-hearings.html (accessed 7 May 2018).

Siwicki, B. (2017), "Machine learning 101: the healthcare opportunities are endless", Healthcare IT News, available at: www.healthcareitnews.com/news/machine-learning-101-healthcare-opportunities-are- endless (accessed 25 May 2018).

Sullivan, T. (2017), "AI, machine learning will shatter Moore's law in rapid-fire pace of innovation", Healthcare IT News, available at: www.healthcareitnews.com/news/ai-machine-learning-will-shatter- moores-law-rapid-fire-pace-innovation (accessed 25 May 2018).

Susha, I., Janssen, M. and Verhulst, S. (2017), "Data collaboratives as 'bazaars'? A review of coordination problems and mechanisms to match demand for data with supply", Transforming Government: People, Process and Policy, Vol. 11 No. 1, pp. 157-172.

Tempini, N. (2017), "Till data do us part: understanding data-based value creation in data-intensive infrastructures", Information & Organization, Vol. 27 No. 4, pp. 191-210.

Winter, J.S. and Davidson, E. (2017), "Investigating values in personal health data governance models", Proceedings of the 23rd Americas Conference on Information Systems (AMCIS).

Winter, J. S., & Davidson, E. (2019). "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance (DPRG), 21*(3), 280-290. Special issue on "Artificial Intelligence: Beyond the hype?" doi:10.1108/DPRG-08-2018-0048

Xiao, C., Choi, E. and Sun, J. (2018), "Opportunities and challenges in developing deep learning models using electronic health records data: a systematic review", Journal of the American Medical Informatics Association, Vol. 25 No. 10, pp. 1419-1428.