Volume 3, Number 1, Spring 2019

Black-box Medicine: protecting patient privacy without preventing innovation

Rhiannon Jackson & Maria McAreavey*

Black-box medicine represents the future of medicine where Big Data and machine-learning meets Big Health. A development of the personalized medicine practiced today, black-box medicine is implicit or opaque, such that doctors and scientists may not know or understand the complex predictions, or connections between datasets, identified by an algorithm. It is impossible to quantify the life-saving potential this development will yield. However, the development of black-box medicine requires the creation and retention of vast amounts of health data.

This article makes the case for a paradigm shift away from individualistic ideas of health data ownership or control. In doing so, it, firstly, asserts the value and relevance of privacy protections in the regulatory framework. Secondly, it aims to identify the overriding flaws of the present regime, inhibiting both the protection of privacy as well as the deployment of black-box medicine. The final endeavour is the

* Law Students at the University of Nottingham and Newcastle University, respectively.

development of potential solutions, building upon the foundations laid by Nicholson-Price in his seminal article 'Black-box Medicine'.[1]

1. Introduction

Black-box medicine refers to the 'use of opaque computational models to make decisions related to health care'.[2] Introduced into legal scholarship by Nicholson-Price, this concept represents the next stage of personalized medicine, in the form of *implicit,* as opposed to explicit, personalized medicine. Space constraints do not allow for a detailed description of the conception of black-box medicine nor of its potential, but an insightful account is provided by Nicholson-Price in his seminal text of the same name. The world is waking up to the opportunities presented by these advances - where Big Data meets Big Health and machine-learning. From former President Obama's state of the Union address in 2015, to statements made by Prime Minister Theresa May declaring her ambition to 'lead the world in the fourth industrial revolution', government leaders are quick to declare their readiness to utilize the technology.[3]

However, black-box medicine presents a problem for patient privacy. Health records have long been considered to contain some of the most private

---

[1] W Nicholson-Price II, 'Black-Box Medicine' (2015) 28 Harvard Journal of Law and Technology 419-467.

[2] W Nicholson Price II, 'Privacy and Accountability in Black-Box Medicine' (2016) 23 Michigan Telecommunications and Technology Law Review 1, 25.

[3] Independent, 'Theresa May says AI revolution will help NHS prevent thousands of cancer related deaths by 2033' (The Independent, 20 May 2018) <https://www.independent.co.uk/news/uk/politics/nhs-artificial-intelligence-ai-cancer-deaths-2033-technology-promise-a8360451.html> accessed 20 May 2018.

information pertaining to an individual, at least in part by virtue of its potential to lead to discrimination or stigma. Yet, in order to harness the full potential of black-box medicine, vast amounts of descriptive health data are required to develop sophisticated algorithms. It is likely that this data, held in unified datasets, will also need to be distributed widely among different actors compounding the problem. Although the public interest in aggregating such datasets is self-evident, it is submitted that this should not be done at the expense of privacy, as is so often suggested in the literature.

Present privacy protections have long been identified as falling short in the context of Big Data and are, again, only exacerbated in this context. The familiar concepts of informed consent and anonymization are frequently employed by legislatures and regulatory bodies and seem an uncontroversial means of protecting individual privacy by enhancing control. However, it will be shown that for too long these individual control or ownership ideas have been equated with, or presided over, privacy protections with the result that those so-called protections either offer no more than an opt-out or are simply illusory. Despite the failings of the regime, it is privacy itself that is criticized as inappropriate. There is a perceptible fear that the protection of privacy will stymy the development of black-box medicine. However, the two need not be mutually exclusive. Thus, although an apparently easy solution, the view that privacy should be sacrificed in the public interest, is a lazy one. Moreover, it is submitted that the inverse is, in fact, true: without effective privacy protections, the public perception would be such that black-box medicine is never fully realised.

Consequently, this essay seeks, firstly, to assert the value and relevance of privacy protections in the regulatory framework. Secondly, it aims to identify the overriding flaws of the present regime, inhibiting both the protection of

privacy as well as the deployment of black-box medicine; the aim of which – improved health care- should be borne in mind. The final endeavour is the development of potential solutions, building upon the foundations laid by Nicholson-Price in his seminal article 'Black-box Medicine'.[4] With the respect to the latter, we suggest that this necessitates a paradigm shift away from individualistic ideas of health data ownership or control.

2. The Privacy Problem

Although health informational privacy is generally lauded as an important value, the pursuit of which is commendable, uncertainty exists as to what it actually means. As distinct from confidentiality or security, the term privacy is used 'to address the question of who has access to personal information and under what conditions'.[5] Confidentiality, safeguarding information gathered in the context of a fiduciary relationship, and security, dealing with the procedural or technical measures necessary to prevent unauthorised access, are interrelated but nonetheless independent concepts. For present purposes, privacy relates to the 'collection, storage and use' of personal health information - as well as to justifications 'under which data collected for one purpose can be used for another (secondary) purpose'.[6]

Privacy issues are necessarily heightened in the context of black-box medicine. As articulated by Nicholson-Price, there are at least four reasons for

---

[4] Nicholson-Price (n 1) 419-467

[5] Institute of Medicine of the National Academies, The Value and Importance of Health Information Privacy, in Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin (eds.), *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* (The National Academies Press 2009) 78.

[6] Ibid.

this. Firstly, the operation of black-box medicine is dependent on vast quantities of data in order to find 'subtle correlations between patient characteristics and medical diagnoses or treatments'. Secondly, the efficacy of such a system is equally dependent on the information collated being comprehensive, in the interests both of non-discrimination and the creation of unified datasets. Thirdly, black-box medicine necessitates the broad distribution of information between different actors; be they 'healthcare providers, pharmaceutical companies, academic and government researchers' or others. A final concern is the continuous generation of new information which is itself in need of protection. The utility of black-box medicine turns on these and thus 'solutions are unlikely to come simply from reducing the amount of information or limiting its distribution'.[7]

The importance of guaranteeing effective privacy protection in this context cannot be understated, not simply from an individual 'rights' perspective, but since public acceptance may well be essential for its development and eventual deployment in the health sector. Unresolved privacy issues could to a large extent inhibit the operation of black-box medicine. Indeed, although privacy is often perceived as an obstacle impeding innovation, it can, in fact, help 'foster socially beneficial activities like health research'.[8] Without suitable safeguards in place, patients may rely on privacy-protective behaviours, such as the withholding of information, leading to inaccurate or incomplete datasets. Data used in the development of any subsequent algorithms for deployment in precision medicine will 'carry with them the same

[7] Nicholson-Price (n 1).

[8] Institute of Medicine of the National Academies (n 6).

vulnerabilities'.[9] It is probable that those with the most scientifically interesting data, would be those most likely to resort to protectionist behaviour if there was perceived to be inadequate protection. According to PWC, seventy-one percent of UK adults believe that it is important for data to be shared for research purposes into certain conditions. However, almost fifty percent of people do not trust new health technology companies with their healthcare data.[10] Further, wider European research has indicated that individuals are 'averse' to the viewing of health information by 'health insurance companies, private sector pharmaceutical companies and academic researchers'.[11] Moreover, efforts to address the regulatory framework must have in mind the need to address public concerns.

3. In Defence of Privacy

As the utility of black-box medicine is increasingly realised, there is a growing trend in the literature to deny the existence of any greater privacy problem at the confluence between 'Big Data' and medicine. The argument is a familiar one: privacy is an unsustainable constraint if we are to benefit fully from the potential of precision medicine and, consequently, the time has come to

[9] Ibid.

[10] Pricewaterhousecoopers, 'Health Records' (*PwC*, 31 October 2017) <https://www.pwc.co.uk/industries/healthcare/patients-voice/health-records.html> accessed 6 May 2018.

[11] Sunil Patel et al., Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European Survey (PACT Project Consortium 2015) 42.

'reconfigure choices' made decades ago.[12] Certainly, the aim to remove obstacles in the way of life-saving development is admirable.

Skopek, for instance, makes a distinction between privacy losses on the one hand, and privacy violations on the other. Although often conflated in the literature, the question whether someone has suffered a privacy loss is one of fact, whereas the question of whether that amounts to a violation remains a legal question. As such, while predictions or inferences generated by a black-box algorithm may entail privacy losses, he considers that it would be 'deeply problematic to treat inferences as capable of violating privacy'.[13] He uses the case of *Kyllo v United States* analogously, wherein the Court held that an inference could not constitute a violation of the reasonable expectation of privacy arising in the context of the Fourth Amendment.[14] Applying this, he suggests that the black-box approach is privacy enhancing insofar as a researcher 'will not look inside the body and discover facts about that person but rather draw inferences and predictions from the outside'.[15] The relevance of this can be doubted since no reasonable expectation of privacy existed in that case given that there was no exposure of intimate details concerning Kyllo's life. The same would not be true in the context of black-box medicine by virtue of the information involved.

---

[12] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run Around Anonymity and Informed Consent' in Julia Lane and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (CUP 2014).

[13] Jeffrey M Skopek, 'Big Data's Epistemology and its Implications for Precision Medicine and Privacy' in I. Glenn Cohen and others (eds), *Big Data, Health Law, and Bioethics* (CUP, 2018).

[14] Kyllo v. United States, 533 US 27 (2001).

[15] Skopek (n 13).

We agree that the privacy losses entailed in the amalgamation of health data should be justified. Nor do we disagree with the view that inferences should not be treated as violations per se – being the very mechanism that makes black-box medicine attractive - but any justifications should have their basis in law – not semantics. It is unsatisfactory to deny the relevance of privacy, simply because the current framework for protection fails in the context of black-box medicine. We submit that this line of thought is based on a misconception of privacy as secrecy or control.[16] The mistake is clearly embodied in the concepts of anonymity and informed consent (frequently relied upon) which, in turn, permeate all aspects of the regulatory landscape. The failure of these concepts is examined below. For present purposes, it is necessary to consider the wider context in which these rules operate. Both anonymization and informed consent are procedural safeguards representing means to an end; the end goal being the protection of privacy. As such, it should be noted that their failure does not equate to the failure of privacy itself. The real disruption is found in *how* we protect privacy. So far 'attempts to deal with new threats draw from the toolbox assembled to address earlier upheavals' and yet it is still privacy – and not our approach to it – that is deemed to fail.[17] The view that privacy is at odds with the distribution or use of all data creates a false conflict from the start and has stunted a more nuanced debate about where – and why - the current framework fails, preferring to sacrifice privacy instead.[18]

In this way, we seek to move away from the normative debate and ultimately towards a practical framework solution. Where are privacy losses,

---

[16] Barocas & Nissenbaum (n 11).

[17] Ibid.

[18] Ibid.

there should be clear justifications and bases in law. Where there is the potential for violations, there should be effective safeguards. We therefore submit that privacy should remain at the forefront of the development of a regulatory framework for black-box medicine.

4. The Current Framework for Protection

In the context of health-care a patchwork of different protections exist in order to safeguard patient privacy. In the United States (US), for example, the privacy of health data is largely regulated by the Health Insurance Portability and Accountability Act 1996 (HIPAA) and the Department of Health and Human Services' implementing Privacy Rule.[19] The Privacy Rule governs covered entities' uses and disclosures of protected health information, with the aim to 'balance the interest of individuals in maintaining the confidentiality of their health information and the interest of society in obtaining, using, and disclosing health information to carry out a variety of public and private activities.[20] Further, the Genetic Information Nondiscrimination Act of 2008 renders the use of genetic information in health-insurance or employment decisions unlawful.

At the European Union (EU) level, protection of personal data is guaranteed both by the Charter of Fundamental Rights of the European Union (CFR) under article 8(1), and the Treaty on the Functioning of the European Union (TFEU), under Article 16(1). These provisions are given further effect in the new EU General Data Protection Regulation (GDPR), which entered into force 25 May 2018. It should also be noted that protection of privacy in both regions is also underlined by an additional element of human rights; with

[19] Nicholson-Price II (n 1), 23.

[20] Stacey A Tovino, 'Teaching the HIPAA Privacy Rule', (2017) 61 St. Louis U. L.J 469, 475.

article 8 of the European Convention on Human Rights (ECHR), for instance, guaranteeing the right to respect for private and family life. The case law of the European Court of Human Rights has expanded the concept to incorporate personal medical data.[21]

Anonymity and informed consent have 'emerged as panaceas' in the frameworks of both regions: having the power to 'open the data floodgates while ensuring that no one was unexpectedly swept up or away by the deluge'.[22] Anonymization presents a 'best-of-both worlds compromise' in which researchers are able to access data for beneficial purposes while privacy is enhanced since individuals are no longer personally identifiable.[23] The procedural protection is employed as a 'get-out-of-jail-free card', enabling valuable information flows to take place.[24] The approach has been to use anonymity to detach the data from privacy protections. Under HIPAA, the de-identification of health information is sufficient to exempt the relevant data from the protections afforded by the Privacy Rule. In a similar vein, Recital 29 of the EU GDPR states that the principles of data protection should not apply to anonymous information which includes *inter alia* 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'.

Where anonymity is not possible or practicable, informed consent subsumes the role of striking the balance between access and privacy. As a natural corollary of autonomy, the rationale behind the concept lies in the idea

---

[21] *LH v Latvia* App no 52019/07 (ECHR 29 April 2014).

[22] Barocas & Nissenbaum (n 12).

[23] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1703-1704.

[24] Ibid.

that 'privacy means control or ownership over information about oneself'.[25] The idea that individuals should have control over their own data seems familiar and uncontroversial. Twentieth century bioethics 'sought to protect the rights of individuals facing binary, us-versus-them challenges', be they in the paternalistic health-care system or clinical research settings.[26] The informed consent of the data subject is central to the EU GDPR, defined therein as 'any freely given, specific, informed and unambiguous' agreement to the processing of personal data relating to him or her, whether as a statement or other clear affirmative action. The concept is not foreign across the pond either. Indeed, the US Precision Medicine Initiative stated that data subjects 'will need to understand the risks and benefits of participating in research, which means researchers will have to develop a rigorous process of informed consent'.[27]

5. Why does the current framework fail?

The problems with anonymity and informed consent are symptomatic of a more systemic issue within the legal framework: namely, the reliance on individualism. As Evans states, individual self-defence 'whether with a consent right or with an ownership right' may be insufficient to protect against twenty-first century risks.[28] When confronted with personalised medicine, whether implicit or explicit, the present regulatory landscape is disrupted by the rise of

---

[25] Barocas & Nissenbaum (n 12).

[26] Barbara J. Evans, 'Power to the People: Data Citizens in the Age of Precision Medicine' (2017) 19 Vanderbilt Journal of Entertainment & Technology Law 243 – 265.

[27] Genetics home reference, 'What are some of the challenges facing precision medicine and the Precision Medicine Initiative?' (*Genetics Home Reference*, April 2015) <https://ghr.nlm.nih.gov/primer/precisionmedicine/challenges> accessed 21 April 2018.

[28] Evans (n 26), 2.

privacy interdependence; challenging the idea that 'people, acting alone, can effectively protect their own interests'.[29] This is an application of what Nissenbaum terms the tyranny of the minority.[30] The situation is clear in relation to genomic data: 'one family member's willingness to share data in identifiable form may reveal information about others who did not consent to data sharing'.[31] The ability to exercise control over your own individual is rendered nugatory when the deeply descriptive data of others has the potential to reveal information about you – even in cases where consent has been withheld. It is possible to foresee this as a lacuna in the law: information innocuously garnered about non-consenting individuals could be utilised outside the scope of protection. As Roger Allan Ford concluded: '[t]oo often, accounts of privacy focus on information subjects, rather than outside who collect, use, and disseminate information.[32]

Unsurprisingly, present data protections endeavor to restrict the amount of information available as a means of safeguarding individuals from unscrupulous uses of personal information. The less data available, the less opportunity for privacy violation. Except in cases of use in order to provide care, the Privacy Rule dictates that 'the amount of information disclosed must be the minimum necessary, preventing most bulk disclosures of information'.[33] Much in the same way, the GDPR requires personal data to be 'collected for specified, explicit and legitimate purposes' (Article 5(1)(b)) as well as 'adequate, relevant and limited to what is necessary in relation to the purposes for which

---

[29] Ibid.

[30] Barocas & Nissenbaum (n 12).

[31] Evans (n 26).

[32] Roger Allan Ford, 'Unilateral Invasions of Privacy' (2016) 91 Notre Dame Law Review 1075

[33] Nicholson-Price II (n 1) 23.

they are processed' (article 5(1)(c)). Yet, as indicated by Skopek, black-box medicine incorporates the use of data 'whose relevance is not known and might never be known'.[34] It cannot be stated *ex ante* what information will be relevant in order to identify life-changing correlations within health data. Further, it may not be possible to state even *ex post facto*, given the opacity with which black-box medicine operates. However, the very utility of black-box medicine lies in its ability to identify what current practitioners and medical researchers are yet unable to identify. To limit data to what current scientific understanding indicates is relevant, would thus be to limit that utility. In the context of the GDPR, it may be suggested that article 5 should be interpreted so as to allow individual data subjects to consent to the processing of their health data with 'exploration' as a specified, explicit, and legitimate purpose.[35] While a means to achieve the aim of removing developmental obstacles, it represents too great a stretch of the legislative language. Such an interpretation would do little to counter the detrimental erosion of privacy protections or the arguments seeking to conceive of privacy irrelevant.

Informed consent is little more than illusionary ideal when applied to black-box medicine. Individuals may grant access to their health data 'too casually' and 'cede control' over subsequent uses of it.[36] With the volume of data necessary to realize black-box medicine on the imagined scale, it would be naïve to expect that each potential data subject would possess the capacity to individually evaluate the protections afforded by a particular developer and

---

[34] Skopek (n 13) 36.

[35] Kees Groeneveld, 'Four ways how GDPR impacts AI' (*Linkedin*, 12 March 2018) <https://www.linkedin.com/pulse/four-ways-how-gdpr-impacts-ai-kees-groeneveld/> accessed 28 April 2018.

[36] Evans (n 26)

make an informed decision as to whether to participate or not. At the same, it is likely that such protections would be framed in terms too broad to be of any real or enforceable meaning. In this way, the 'take-it-or-leave-it right to refuse'[37] either fails insofar as it incorporates individuals in research whose consent is no more than token or insofar as it fails to garner the data of enough people so as to realise the promise of black-box medicine. With respect to the latter, it has already been suggested that there are 'strong ethical objections to making life-saving health research depend on individual choice to use information'.[38]

Even if the failure of informed consent cannot be accepted, it is nevertheless the case that individual choice, even where effectively executed, is 'not the same' as privacy protection such that 'merely providing choice does not necessarily enhance privacy protection'.[39] It is only really in the instance that consent is withheld that privacy will be effectively protected. The existence of effective protections themselves may make a person more likely to grant their free and informed consent, and thus provide some incentive to developers to pursue such safeguards. Yet an individual, having so consented, will not find any protection in the act of consent itself. Such a view relies on the fiction of informed individuals equipped to tackle legalistic language, likely at some length. As above, it is untenable to promulgate that fiction at the expense of individual rights. There are further issues with respect to the ownership of data, as will be explored below.

---

[37] Ibid.

[38] Fred H Cate, "Protecting Privacy in Health Research: The Limits of Individual Choice" (2010). Articles by Maurer Faculty. Paper 235. http://www.repository.law.indiana.edu/facpub/235

[39] Ibid.

The 'anonymization assumption'[40] - the belief that the detachment of personally identifiable information is an effective privacy protection - is problematic in two ways. Firstly, the possibility of being able to re-identify someone increases with the amount of information available. The volume of literature exploring this issue means detailed discussion of it is beyond the scope of this article Nonetheless, it is beyond doubt that '[d]eeply descriptive data display the irreproducibility of each of our like trajectories'.[41] The removal of explicit identifiers is a weak protection against the specificity of an electronic health record which has recorded data over the course of a subject's life. To take Evans' example: there may only be one person who 'cracked the upper right incisor at thirteen years… while giving birth to healthy daughter at twenty-six years… and developing dementia prematurely at the age of fifty-three'.[42] It can therefore be said that the distinction between personally identifiable and non-personally identifiable information is something of a false dichotomy.[43] The situation is even clearer if one includes lifestyle data, such as the number of steps walked on a specific day, within the scope of a particular dataset. Indeed, in 2016, 165,000 such apps were available for download on Apple's iOS and Google's Android operating services.[44] Secondly, de-identification is undesirable insofar as it makes the creation of unified datasets more difficult or impossible. The more comprehensive the 'greater capacity to tease apart complex implicit

---

[40] Ohm (n 23).

[41] Evans (n 26) 2.

[42] Ibid.

[43] Cate (n 32).

[44] The Economist, 'Things are Looking App' (*The Economist*, 10 March 2016)<https://www.economist.com/business/2016/03/10/things-are-looking-app> accessed 01 June 2018.

relationships'.[45] Moreover, it has also been suggested that, as a result, 'deidentification can act as a false security blanket, reassuring individuals that privacy risks are lower than they are'.[46]

It is now evident that the framework fails not only to advance the public interest, but also to protect the individual. In the context of medical research, criticisms of privacy protections have been common. As aforementioned there are 'ethical objections' to conditioning life-saving research on individual choice, although it is continually employed to reinforce privacy rights.[47] It has been suggested that requiring individual consent can have a 'chilling effect' on participation.[48] A comparison of pre- and post-HIPAA consent demonstrated a decline in consent from 96% to 34% respectively.[49] Moreover, individuals may consider repeated contact by researchers to be intrusive or a breach of confidentiality, especially where access to 'de-identified' data is sought.[50] It is also logical to expect participation to be less where individuals are contacted regarding studies they do not consider salient to their own health.[51] In this way, it is problematic to rely on individual altruism in order to advance the public

---

[45] W Nicholson-Price (n 3) 20.

[46] W Nicholson-Price (n 1) 34.

[47] Cate (n 32).

[48] Ibid.

[49] Armstrong D, Kline-Rogers E, Jani SM, Goldman EB, Fang J, Mukherjee D, Nallamothu BK, Eagle KA. Potential impact of the HIPAA Privacy Rule on data collection in a registry of patients with acute coronary syndrome. Archives of Internal Medicine. 2005;165(10):1125–1129

[50] David Casarett et al., Bioethical Issues in Pharmacoepidemiologic Research, in PHARMACOEPIDEMIOLOGY 593 (Brian L. Strom ed., 4th ed. 2005).

[51] Sandra Galea & Melissa Tracy, 'Participation Rates in Epidemiologic Studies' (2007) 17 Annals of Epidemiology 643–653.

interest in developing algorithms in black-box medicine. Low rates of participation, in turn, risk selection bias. This will occur when differences exist between those who consent and those who do not consent to the use of their data for black-box purposes. Numerous studies have examined whether the HIPAA's Privacy Rule has led to bias in research. Authorisation requirements thereunder have been found to act as a deterrent for African American participation in research, with consenting patients more likely to be older, married and white.[52]

However, these criticisms are not new. Perhaps the turning point in encouraging change is the fact that the focus on individual control is now failing to protect even the individual with 'control' over their data. Privacy interdependence means that 'individuals cannot, through their own autonomous decision making, protect their own interests anymore'.[53] One might expect that regulatory change will be more ardently supported in light of this fact, since it is no longer necessary to justify reform solely on the basis of utilitarian ideals about what is in the public interest. For too long the answer to the aforementioned problems has been to 'try harder, to be more creative' and to adopt more sophisticated techniques.[54] It is submitted that a paradigm shift in thinking about privacy is necessary.

6. Solving the Problems

In order to guarantee protection of privacy at all times, it may be necessary to distinguish between two different, but interrelated, stages where problems arise. Firstly, there are the issues arising in regards to the initial development of black-

[52] Baroccas and Nissenbaum (n 13).

[53] Evans (n 26).

[54] Baroocas and Nissenbaum (n 12).

box medicine. The most significant concern here is almost certainly the generation of datasets on such a scale as to be able to permit the operation of black-box medicine and to minimise the risk of selection bias. Secondly, there are the issues arising from the *operation* of black-box medicine. Solutions in respect of these will need to address Nicholson-Price's fourth concern, namely, the constant creation of new information in need of protection.[55] Of course, many protections will be relevant to both stages but it is nevertheless beneficial to have in mind the possibility of differentiation where unique problems arise.

7. Academic Solutions – Will they work?

It has been made clear that there are significant challenges for the protection of patient privacy within black-box medicine, with the current framework still expressing inherent structural weaknesses. Nicholson Price has developed a framework for establishing a solution that seeks to enable the protection of patient medical data in the realm of Black Box Medicine. He focuses on 'protecting patient privacy while permitting data to be used for algorithmic verification'[56] without impinging on accountability. This can be developed further below alongside Evans, Schneider and Solove who form their own solutions to the challenges of Black-box medicine.

Nicholson Price focuses on 'substantive restrictions on data collection, use and disclosure'[57], and emphasizes the importance of protecting privacy whilst promoting accountability. His proposal confronts the lack of incentive to ensure vast data collection is cultivated and utilized legitimately. Price points to the use of structured systems where a 'third party submits test algorithms to an

[55] Nicholson-Price II (n 1).

[56] Ibid.

[57] Ibid, 31.

interface offered by a data collector and receive outputs based on patient data – without receiving that specific patient data'[58]. His argument therefore emphasizes that the ability to maintain sensitive data must be highly regulated and not roam within the free market for all to access.[59]

However, Prices' argument is weak as he fails to note that there are inherent legal structures and regulatory devices that already exist. Price fails to explain why an 'elaborate array of new regulatory devices are fully needed'.[60] Carl Schneider presents a stronger argument to suggest that importance lies upon utilizing regulatory instruments that the law already has to adapt to the emerging field of Black-box medicine and protect patient privacy.[61] This is highly credible through practicality and supports the argument that many of the privacy issues Price notes are problematic in the field of medicine already, rather than Black-box medicine singularly. Thus, Schneider presents a more pragmatic approach that more should be done with existing regulatory medical privacy issues to further the expansion of this field. This would be more effective than using devices unfamiliar to the developing field of Black-box medicine.

Nicholson Price's further discusses 'Independent gatekeepers governing access to patient data and black box models'[62]. The argument puts emphasis on privacy without regulating algorithmic medical products, such as the HIPPAA privacy rule, which would ensure the disclosure of data - leaving algorithmic

---

[58] Ibid.

[59] Julian James Stephen et al., Practical Confidentiality Preserving Big Data Analysis (first edn, 2014).

[60] Carl E. Schneider, 'A Comment on Privacy and Accountability in Black-Box Medicine' (2017) 23 Mich. Telecomm. & Tech. L. Rev 321, 324.

[61] Ibid.

[62] Stephen et al. (n 59)

certification to the FDA or another 'un-specified entity'.[63] It is apparent through this explanation the importance of before making specific uses of patient data, or disclosing this, an independent gatekeeper should balance patient privacy interests with the need for verification and the expansion of this field.

However, although having persuasive foundations, pulling on the FDA's drug approval process as a fundamental model, Price's solution here lacks structure and development.[64] Price fails to address how to secure this information vs the interests of expanding black box medicine. Barbara J Evans correctly points these interests out as an essential in this developing field. [65] Solove provides a further stronger solution, maintaining that it is 'virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding'.[66] Solove's approach is highly convincing as he pragmatically notes how it is important to elaborate further on how black-box medicine can ensure complete security for patients when choosing to submit their private data.

Furthermore, it is important for commentators to focus on informed consent with patient data and how this can still be achieved when balancing such interests with the progression of Black Box Medicine. The Institute of Medicine, uses this as an essential in the collection of data, particularly in when volunteer data sets have been assembled for no other reason than algorithmic development. Many believe it is a right to choose where their own data is

---

[63] Ibid.

[64] Ibid.

[65] Barbara J Evans, 'Much Ado about Data Ownership' (2012) 35 harvard journal of Law and Technology 69, 93-94.

[66] Daniel J. Solove, 'Privacy Self- Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

accessed. This would not be effectively processed unless it was the owners (the person) determining when and in what conditions the researchers can get access to patient data. Despite this, requiring this 'individual consent' is time consuming, impractical and imposes significant obstacles in the advancement of Black-Box Medicine and other methods are more plausible when ensuring security of patient data and black-box medical models, a 'fairytale'[67] ideal. Clinical research suggests relying on patient consent will create undue biases, as patients willing to consent differ from those who are not.[68] Solove[69], rightfully argues that it is 'virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential down steam uses'[70], something that is lacking an education. Indeed, these complications exist with clinicians today, but the promise of Black Box Medicine is to be one that can solve complex data issues, holding vast amounts of information, thus helping advance the field of medicine.

Price's third solution is 'Information Security Requirements'[71]. This discusses the governance of the storage and passing of medical information. This argument is designed to avoid losses due to a breach instigated by third parties. It further develops that access should be 'limited to those individuals with legitimate needs and should be highly person-specific so access can be followed

---

[67] Ibid, 1890.

[68] Gordon B. Moskowitz, Jeff Stone and Amanda Childs 'Implicit Stereotyping and Medical Decisions: Unconscious Stereotype Activation in Practioners' (2012) 102 American Journal of Public Health 996.

[69] Solove (n 66).

[70] Ibid, 5.

[71] Nicholson-Price II (n 1).

and withdrawn'[72]. He puts emphasis on the use of a 'two-factor authentication instead of simplistic password system'[73], and discusses the updating of these techniques on a regularity to ensure they are sufficient and reliant.[74]

However, although this is persuasive when dealing with this on a security basis, his approach fails to collectively recognise the quantity of data that dealt with in the expansion of Black Box Medicine. Price bases his third pillar on the Federal Trade Commission and its reliance on 'quasi-common law enforcement of reasonable security standards'[75]. Although this approach is idealistic, it fails to consider the mass amount of data that is being represented in this field. His argument does not show any real basis on how these requirements can work, but is highly simplistic based on older practice, prior to an expansion within the field of Black Box Medicine. This would perhaps exhibit a fear of going back to outdated methods of individual data ownership, when using larger amounts of data, as such existed in twentieth-century informed consent requirements. Brent Mittelstadt correctly argues that this form of ownership, supplies 'too many duties and limitations when expanding this field'. [76] This is merely a premise that cannot be successfully carried through. Thus, is not expanding alongside this modern and developing field within Black-Box Medicine.

---

[72] Ibid.

[73] Ibid.

[74] Ibid.

[75] Ibid.

[76] Brent Mittelstadt, '*From Individual to Group Privacy in Biomedical Big Data*' (Cambridge University Press 2016), 178.

8. Independent gatekeepers – a fear of 20th century outdated rulings on privacy

Although privacy has failed to change much since the 1970's, there has been an inherent focus on the concept of informed consent, which as mentioned previously, is an outdated concept when dealing with Black Box Medicine. The Institute of Medicine discusses the impossibility of eradicating patient consent, however, Daniel J Solove in Privacy Self-Management and the Consent Dilemma[77], states that the 'law provides people with a set of rights to enable them to make their own decisions about how to manage their data' known as 'privacy self-management'[78]. This explanation suggests in the field of Black Box medicine we must enable people to make their own individualistic decisions on their private data as it is something to what they should be able to own, regulate and make decisions on themselves.

However, as implicitly stated before this is something of a fictional concept. To contrast Solove's single statement here, Evans makes an expansion on this field by developing and notifying an understanding of there being 'too many large entities for this to be sustained in the developing field of Black Box Medicine'[79]. This would imply that it is indeed highly fictional to manage privacy separately when assessing the use of patient data within Black Box Medicine on a patient to patient individualistic and autonomous basis. Cohen supports this through notifying that 'innovation relies on privacy which is

---

[77] Solove (n 66), 1891.

[78] Ibid.

[79] Barbara J. Evans, '*Big Data and Individual Autonomy in a Crowd*' (Cambridge University Press 2017), 22.

increasingly under threat'[80], particularly with the advancement of Black Box Medicine[81]. Thus, to expand this further, for Black Box Medicine to be able to advance, we must advance security and privacy laws in this field alongside this, as two parallels within the field, using a stricter and more cohesive process. Cohen strengthens this view further, maintaining how the implications privacy and how this fosters a 'certain kind of society'[82]. Therefore, it appears highly practical to bring ideas together for collective action.

Since it has been identified that people's decisions about their own privacy can affect society and the progress society makes, this leads to the natural assumption that a societal change or collective and group change is needed to successfully address the privacy and security issues we are faced with under the expansion of Black-Box Medicine. This would suggest a lead from an individual autonomous approach of large data, to this being in a used collectively within a group of individuals. This is a concept discussed by Barbara J. Evans that will now be expanded upon as being a more successful method needed in the expansion of Black-Box medicine.

9. Collective Medicine

Presently, autonomy is an individual's power and authority to make decisions and act alone. This is unsurprisingly a fictional concept in the changing nature and expansion of Black-Box medicine. Therefore, solutions may lie in collective action and group privacy. Through this method, the discussion of patients would enable individuals who are wanting to know and discover more about the

---

[80] Glenn Cohen et al., Big Data, Health Law, and Bioethics, '*Medical Malpractice and Black-Box Medicine*' (2017) 4.

[81] Ibid.

[82] Ibid.

privacy of their health data corresponds with the need for an advancement in black box medicine, particularly when dealing with large scientific data. [83] This is important to ensure that a patient's autonomy is protected, yet the advancement of modern medicine is not hindered.

Black-box medicine ensures the holding of large amounts of data for millions of people. To reduce bias and error as discussed previously, a potential solution to this is forming population sub-groups and the concept of collective data, where data is collected from individuals and then used and collaborated as a whole.[84] Evans presents the convincing argument that individuals are making too many negotiations on their own data and privacy, and are not being successfully provided with an explanation in a new and expanding field thus this may offer a more convincing solution.

The traditional informed consent norms of the Common Rule and the HIPPAA Privacy Rule, were designed decades ago purposefully for clinical research and studies with smaller amounts of data. Indeed, although effective for these small sets of data, this form is not adequate when dealing with the new social challenges and issues with privacy and security that black box medicine brings as it cannot go far enough to respect patient privacy. Thus, collective action or individual autonomy within a group is more persuasive. Evans however argues that 'some value their individual autonomy so greatly, and these people may be more unwilling to work with other people to pursue public health objectives'[85]. Evans is correct, supporting that 'this concept may change if these individuals were willing to cooperate with other people if that were to be the only way

[83] Evans (n 79) 20.

[84] Ibid.

[85] Ibid.

to protect their own individual privacy',[86] thus offering a more promising solution to this challenge.

However, this common purpose requires solidarity and a need for conformity in communities. Richard Rorty reflects on a historic struggle to reconcile individual autonomy with membership in a community[87]. This therefore brings into question thus whether society is developed enough today to be involved in future developments in this field. Conflictions are apparent in society today with people being deeply divided about privacy, security, laws and ethics, making solidarity and collective effort something difficult to achieve. To expand further, an idealistic solution of a deeper and more broad education of people on the effectiveness of collective action and sub-group analysis and work on data in the medical field. Although not a quick and short solution, the field remains something to the ordinary person that is indeed a 'black box', which in many case does cause hostility, reluctance and an unwillingness to divulge their own data, if it is of something they are not well educated on or aware of the security or privacy involved in the process.

However, an inherent difference lies in those individuals who feel the need to obtain complete control and access over their own health data and those who believe their data should be available to serve public good and development. However, Brent convincingly argues that full privacy is an 'unrealistic ideal'.[88] Despite this, the concept of freely giving medical data for a field that is emerging and continuously developing is still fearful for many individuals.

---

[86] Ibid.

[87] Richard Rorty, *Consequences of Pragmatism*, 1992 (first edn) 1972.

[88] Mittelstadt (n 75).

10. Will this collective approach work?

Evans further discusses the importance of groups being collectively formed in society being able to 'enunciate their own decisions with their own and their member's data, with first obtaining their own health data by exercising their HIPAA section 164.525 access rights'.[89] This is significant when moving away from the concept of informed consent. Expanding on Evans, this is an essential movement needed as it transgresses away from the outdated concept of the 20th century belief that informed consent is protecting people's privacy and security, when in fact it is not. However, Evans is insistent that this concept is not a panacea,[90] but enables people to get involved in their own biological ethics and choices, and brings a needed switch from individual autonomy to a social consciousness[91] and enables education of these current issues.

11. Going further: a Duty to Share Health Data?

Glenn Cohen has argued in favour of a duty to share healthcare data. Such a duty would remove the obligation to obtain consent in many instances where data from electronic health records (EHRs) are required to improve healthcare: in this instance, and for present purposes, the development of black-box medicine.[92] It represents a clear means of assembling the vast data resources that twenty-first-century medicine requires, which may not otherwise be possible.[93] In Cohen's view, imposition of the duty can be defended along two different

---

[89] Ibid 26.

[90] Ibid.

[91] Ibid.

[92] Glenn Cohen,' Is There a Duty to Share Healthcare Data?' in *Big Data, Health Law, and Bioethics* (Cambridge University Press 2018).

[93] Evans (n 26).

argumentative pathways: namely, that '(1) healthcare data are not the patient's property and (2) sharing the healthcare data fulfils obligations of reciprocity'.[94] The latter encompasses the idea that those who benefit from medical innovation based on EHRs should also contribute. This can be supported as an uncontroversial embodiment of the public interest idea; it is the first argumentative pathway that represents the biggest hurdle to acceptance. However, as we have already indicated, there are reasons to doubt the value of ownership or control (consent) ideas in the protection of privacy.

Informed consent has been employed as a procedural device under the assumption that it will protect privacy. As technology enables the movement towards implicit personalized medicine, the current consent-focused framework is revealed to be based on a fiction. It would be inappropriate to continue to propel this fiction at the expense of advancing medical science in the form of implicit personalized medicine. Consent is not privacy and nor is it an effective means of protecting it. At best it offers an opt-out in the event that substantive privacy protections are insufficient. Thus, issues lie in public perception of privacy than any other. Despite the recognized failings of individualism, it is certainly hard to conceive of 'self-serving individuals, endowed with the right to make autonomous decisions that serve their own perceived best interests' willingly surrendering that right – however illusory - in favour of a scheme of common purpose.[95] Furthermore, it should not be a requirement for these individuals to do so.

Indeed, Evans states that, 'ethically repugnant to many people', compulsory data access has not been, and may never be, embraced as a 'general

[94] Cohen (n 56).

[95] Evans (n 26).

solution' to the problem of making data available for research.[96] However, it has not been suggested that any duty to share health data should be applicable generally. The duty is context-specific and thus operational only within strict constraints. The duty Cohen envisions is limited to health care data, as opposed to data about one's health (which might include, for instance, an individual's step count) and is further limited with respect to the data user. Governmental agencies tasked with improving health care and hospital systems with similar goals represent the two 'ideal types' of user, largely due to their key role in advancing the public interest. Purely private companies (perhaps with the exception of hospital systems, as stated) are not owed any duty by data subjects, and nor do they obtain unfettered access to the resulting data simply by virtue of its existence. The view of the duty as morally questionable is pre-occupied with privacy as secrecy and control which we suggest has led us down the wrong regulatory path, effectively minimizing privacy protection.

It is possible to foresee broad conceptual differences in the implementation of such a duty between the US and EU. It is possible to argue that compulsory data access integrated into a scheme of universal health care, as is more prevalent in Europe, is much less controversial. For instance, allowing the patient data held by the UK National Health Service (NHS) to be used in the development of algorithms within the relevant parameters instinctively feels instinctively less problematic than necessitating the sharing of data with a private provider of health care. A legislative duty does not seem morally *ultra vires* when the provision of health care is conducted as part of a comprehensive public service. As acknowledged by the UK House of Lords, while individuals do not like the idea of the NHS selling data, they dislike more the idea of private

[96] Ibid.

companies making a profit at the expense of both the NHS and its patients.[97] As such, a duty to share may be necessary to keep the service from falling irretrievably behind the times. On the other hand, if one wishes to avoid compulsory access, then there is likely more opportunity to do so under the notion of freedom to contract. Individuals could, for instance, opt for a private provider which chooses not to impose such a duty. Such a switch would be more difficult to effectuate in public health care schemes, but relies heavily on socioeconomic possibility.

However, if it is accepted that a duty to share health data can be imposed in a way that does not infringe privacy (as we suggest is the case), then it may be possible to gradually expand the duty to private developers who can make specific and enforceable guarantees of the same privacy protections as would be required of public service providers. As Cohen states, hospital systems, although private, would perhaps be an early example of this. Cohen has significant strengths to his argument such as the duty to share health care, because consent (as argued above) is not effective in protecting patient medical data anyway. However, it is still problematic as to whether there is enough security currently in place for Cohen's argument to become a reality.

12. Conclusion

While the literature in this area remains in its relative infancy, it is not possible to provide concrete answers to the questions raised about privacy in the context of black-box medicine. Nevertheless, it has been argued that a paradigm shift is

---

[97] House of lords, 'AI in the UK: ready, willing and able?' (*UK Parliament*, 16 April 2017) <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10002.htm> accessed 12 April 2018.

needed to provide effective protection of privacy in the context of black-box medicine. Scientific progress necessitates a move away from outdated approaches to patient consent, privacy, and security. Traditional regulation by the HIPPA, FDA and other bodies, although fit-for-purpose on the regulation of small data quantities, do not sufficiently fulfill the requirements needed today under modern algorithmic medicine.

The solutions so far proposed also fail to adequately address the weaknesses of the present framework for protection of patient data. As aforementioned, this is clear in relation to the application of informed consent in its traditional form to black-box medicine, whether in relation to the collection of data or its subsequent use. Additionally, although Nicholson-Price emphasizes the importance of privacy, his framework does not go far enough to effectively protect patients. Without further development, his three-pillar approach risks reinforcing the traditional approach to privacy protection that has already been acknowledged as inadequate and even inappropriate. Such a consequence would be detrimental for the development and expansion of Black-Box Medicine.

Group privacy presents a more modern and convincing approach to confronting the challenges to medical privacy as discussed in this article. This is supported by Cohen who notes the importance of a duty to share health care in order for such a developing field to advance. This is significant as currently the concept of consent is something of a fiction to the individual, shown throughout this essay as something unsatisfactory. It is important to note however that focus should lie on enforcing security with large sets of data and using legal means to do so, to ensure that this is not sacrificed in the process.

In the age of big data, public health and privacy are collective enterprises that must run in parallel in order to be successful. Until an essential shift from

individual autonomy towards the idea of social consciousness[98] is negotiated, it appears that either privacy or innovation will be sacrificed at the hands of the other. More work should be done to focus on developing a framework that strikes at the right, or publicly acceptable, balance between the two.

[98] Evans (n 79).