The Use of Data Mining by Private Health Insurance Companies and Customers' Privacy

An Ethical Analysis

YESLAM AL-SAGGAF

Abstract: This article examines privacy threats arising from the use of data mining by private Australian health insurance companies. Qualitative interviews were conducted with key experts, and Australian governmental and nongovernmental websites relevant to private health insurance were searched. Using Rationale, a critical thinking tool, the themes and considerations elicited through this empirical approach were developed into an argument about the use of data mining by private health insurance companies. The argument is followed by an ethical analysis guided by classical philosophical theories—utilitarianism, Mill's harm principle, Kant's deontological theory, and Helen Nissenbaum's contextual integrity framework. Both the argument and the ethical analysis find the use of data mining by private health insurance companies in Australia to be unethical. Although private health insurance companies in Australia cannot use data mining for risk rating to cherry-pick customers and cannot use customers' personal information for unintended purposes, this article nonetheless concludes that the secondary use of customers' personal information and the absence of customers' consent still suggest that the use of data mining by private health insurance companies is wrong.

Keywords: privacy; data mining; health insurance industry; private health insurance

Introduction

Private health insurance (PHI) companies collect massive amounts of personal information about their customers. Data mining allows these companies to segregate customers into categories of which the customers themselves are unaware.[1] Data mining also allows these companies to cherry-pick customers,[2,3,4] making the use of this technique within the PHI industry an area of major privacy concern.[5] The literature on the ethics of healthcare data mining, however, is predominately American. PHI companies are not regulated elsewhere in the same way they are in the United States. Private health insurance companies in Australia are tightly controlled by the government, and the privacy laws pertaining to the industry differ from those in the United States, where PHI companies can set the price of their products based on an assessment of the individual customer's risk. Understanding how data mining is used by PHI companies outside the United States, particularly in developed nations like Australia, is therefore of potential significance, particularly if it raises privacy issues. Of particular interest is the role of privacy protection laws in protecting customers from potential misuse of information arising from data mining.

The author wishes to thank the Faculty of Business at Charles Sturt University for funding this study, Deborah Munns (Charles Sturt University) for her assistance with the literature review for this article, and Kathryn French (Charles Sturt University) and Mary Rorty (Stanford University) for editing earlier drafts of this article.

Cambridge Quarterly of Healthcare Ethics (2015), **24**, 281–292.

doi:10.1017/S0963180114000607

Using the Australian PHI industry as a case study, this article explores the implications of the use of data mining for the privacy of the customers of PHI companies. Classical philosophical theories, specifically utilitarianism, Mill's harm principle, Kant's deontological theory, and Helen Nissenbaum's contextual integrity framework, are then invoked to arrive at a judgment about the ethical implications of the preceding argument.

Data Mining in the Context of PHI

When consumers apply for private health insurance, the insurers collect personal information like age, gender, geographic location, and marital status. The classifications or categories generated from data mining are based on this nonsensitive information and consequently would not seem to directly violate privacy. Data mining is a process of searching within large datasets in order to reveal unpredicted correlations, which might then allow the companies to place customers in new and nonobvious classifications, categories that the customers might not have imagined applied to them. The newly discovered classifications are generated on the basis of inference from the vast amounts of individual personal information within larger datasets. As the records of new customers are added to the databases, data mining can suggest the relevance of these discovered classifications or categories.[6] But because, in reality, the included customers may not actually fall into the discovered classifications or categories, the criteria used for assignment may not be appropriate.

Data mining is a well-established practice in many fields, including marketing, advertising, finance, banking, and insurance.[7] Data mining utilizes various techniques such as classification, clustering, association rule mining, and summarization of data, making it possible to discover trends within the data, extract meaningful information, and predict the value of future data. In addition, new information generated as a result of data mining techniques can provide businesses with accurate "profiles" of consumers and their purchasing behavior, allowing them to more effectively target their customers. This makes data mining an indispensable tool for marketing purposes.[8]

However, profiling through data mining can lead to some de-individualization. People are treated as group members, rather than as individuals—which makes it possible for people to be labeled and discriminated against or stigmatized.[9] Karpurika Raychaudhuri and Pradeep Ray note that privacy is especially important for PHI customers if they suffer from a stigmatized illness.[10]

Data mining in the context of health insurance has proven to be effective in detecting fraud.[11] In the United States, the cost of fraud in national insurance was estimated in 2003 at $170 billion. When a health insurance company in the United States built a data mining application to detect fraud, it led to savings of $11.5 million in one year alone. Data mining can be used to detect underdiagnosed patients, thereby avoiding expensive claims. Data mining can also be used to detect high-risk customers, giving health insurance companies the opportunity to plan appropriate intervention and prevention strategies. However, data mining does involve the secondary use of personal information, which is one of the areas of major privacy concern. *Secondary use* is when information provided for one purpose is used for an unrelated purpose. Corey Angst notes that information gleaned from linked databases can be used in new and unanticipated ways, often without the knowledge

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

of customers.[12] The data could also be linked to other databases as a means of generating new information, which in turn could be used in the future for applications that may not yet be fully developed.

Raychaudhuri and Ray argue that electronic personal information has the potential to be easily duplicated and shared with others who are not party to the original disclosure, often without the individual's knowledge. Shaheen Borna and Stephen Avila add that this information may eventually be used by a number of other interested parties, such as potential employers.[13] Raychaudhuri and Ray concur, adding that data may include information about physical health, genetic information, information on mental health, and much more. Information from data mining may influence employment and employability, credit worthiness, and one's ability to get health insurance—in some cases it may affect the rates paid for coverage.

Proponents of health information exchange argue that customers' information is usually stripped of all identifiers prior to being mined. Privacy advocates, however, argue that simple automated methods can be used to reidentify customers' data by cross-referencing using the data available from public sources, such as voter registration databases. Lita Van Wel and Lambèr Royakkers argue that even nonidentifiable data can become identifiable when different sources are merged together.[14] Proponents of health information exchange argue that linked databases can save costs by eliminating duplicate services, improving care, shortening hospital stays, and streamlining treatment and care among all care professionals and geographic locations. They add that a massive database of health information would allow for improved public health reporting, bioterrorism surveillance, quality monitoring, and advances in clinical trials. Health information exchange can also help businesses target new customer groups through marketing segmentation, minimize their costs, and sell more products.

Data mining can be used to identify individuals on the basis of value. That is, data mining can be used to classify consumers based on an estimated or predicted valuation of their economic circumstances. It can then be used to impose price discrimination, in which the same good is offered to different consumers at different prices, or to restrict access to goods or services. This doctrine of "fair discrimination" holds that an insurer has the right to measure the burden of the policyholder on the insurance fund, and to charge appropriately for it. Thus consumers with different risk factors will bear different costs for their insurance. Proponents of data mining in PHI argue that insurance costs will rise for all if insurance companies are not sure of the "true" risk they need to underwrite. Privacy advocates, however, argue that using data mining techniques in this way can encourage businesses to engage in discrimination against their customers.[15] Data mining has the potential of allowing insurance companies to cherry-pick only those people who are healthy and require fewer health services. Privacy advocates argue that if insurers, for example, use genetic testing, then insurance will only be affordable to those people deemed to have "healthy" genes. Those with "defective" genes may be subject to higher premiums or, at worst, may even be denied insurance coverage. The respondents to a public opinion survey conducted by Borna and Avila raised these concerns.

The use of data mining can also be problematic with respect to informed consent, which relates to notice (being aware) and consent (having choice). A person whose information is being collected may not be aware that his or her information is being mined, does not know how the results will be used, and has no opportunity to consent to the uses or to withhold the information. Privacy advocates argue that projects that rely on individuals voluntarily forfeiting certain elements of their private information are misleading, as most nonexpert participants could not have a full understanding of what opting-in means, because the possible uses of the information are still evolving. A further challenge of data mining is that it is often not clear what patterns will be revealed from the data. This would make it impossible to clearly specify in advance the exact purpose of data collection in order to notify the data subjects. As far as customers are concerned, Donald Willison et al.[16] found that customers want their consent to be sought before their personal information is used for a second purpose. Insurance companies, on the other hand, say that if individuals are concerned about their privacy, they should refrain from purchasing insurance policies.

The issues surrounding customer privacy are further complicated by the absence of laws regulating data mining. Herman Tavani argues that the current privacy laws do not offer individuals any protection for how information obtained through data mining will subsequently be used.[17] This is particularly problematic if making decisions about who can become a customer is conditional on categories discovered by data mining.

The Australian PHI and Privacy Laws in Australia

PHI in Australia is provided by private health insurers registered under the PHI Act of 2007.[18] The operations of all registered private health insurers are monitored by the PHI Administration Council (PHIAC), an independent Australian government body that ensures that the insurers are able to meet their financial obligations to their customers. By law, private health insurers cannot and should not engage in risk rating, in which a price set on an insurance product is based on the likelihood of an individual making a claim. Private health insurers instead must follow a principle known as "community rating." According to this principle, everyone is entitled to buy the same product at the same price,[19] and health insurers cannot offer different prices according to age, gender, state of health, or the size of one's family. Life insurance, trauma insurance, and disability insurance can be risk rated, however. The PHIAC gave the following example: "A single, healthy 20 year-old and a single, unwell 60 year-old will both pay the same premium for the same cover [from the same insurer]. However, the cost of premiums for similar cover may vary between insurers." In addition, private health insurers cannot refuse to insure a customer, and everyone also has the right to have their policy renewed by their private health insurer.

The PHI Act of 2007 also regulates the gathering and disclosure of customers' personal information by private health insurers. All PHI bodies in Australia, including Private Heath Care Australia, the PHIAC, PHI Ombudsman, and Consumers Health Forum of Australia, must comply with the national privacy principles set out in the Privacy Act of 1988. The Privacy Act of 1988 sets out clear rules about information handling, including how businesses may collect, use, store, and disclose personal information. In addition, the Healthcare Identifiers Act of 2010 provides an additional layer of protection for PHI customers' personal information. The act contains clauses that exclude the use of the healthcare identifier of a healthcare recipient for the purpose of communicating or managing health

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

information as part of a contract of insurance for the healthcare recipient.[20] However, the Privacy Act of 1988 does not adequately protect customers' records from nonconsensual secondary use of data, such as data mining. The information privacy principles (IPPs), which apply to businesses with a turnover of three million dollars or more, do not explicitly mention the threats of data mining to privacy. But the IPPs do state that personal information shall not be used for a purpose to which the information is not relevant, meaning that using personal information for purposes other than those for which it was originally gathered and intended is against the law.

The Research Approach

The Empirical Component

The aim of this study is to explore the implications of data mining for the privacy of customers of PHI companies in Australia. To achieve this aim, qualitative interviews with key experts were conducted during the months of July and September 2013 and February 2014. The data from these interviews were analyzed immediately after collection.

In addition, a search of Australian governmental and nongovernmental websites relating to PHI was conducted in October 2013. The terms or keywords used were obtained after a comprehensive literature review conducted in January 2013. More than 10 governmental and nongovernment websites were visited. The results from the qualitative interviews and the searches of Australian websites are incorporated into the subsequent argument.

The Philosophical Component

To develop the argument, critical thinking software frequently used for argument mapping was employed. This technique is widely used in work in the fields of information technology ethics, English, social studies, history, and philosophy and has been adopted by several universities in Australia. Argument mapping is a philosophy-based method of representing ethical problems and working toward logical arguments and is effective in representing ethical arguments diagrammatically.[21] Argument mapping is useful in formulating well-reasoned arguments and writing clear and concise essays, so long as the diagram is developed before the essay is written. The program Rationale, provided by Austhink Software, was used to develop the argument map. This program helps to build a model of the argument, allowing the user to clearly see the logical structure. The developed argument can then be converted into an essay and can be used as a basis for making a moral judgment about the ethical issue raised.

First, a diagram was constructed using Rationale to map the argument, presenting the main premise and the supporting reasons for it and objections to it, with the intention of developing a rational argument. Then the diagram was converted into textual form, adhering closely to the generated map of the argument. Finally, four philosophical formulations—utilitarianism, Mill's harm principle, deontology, and contextual integrity—were applied to the main premise of the argument to arrive at a moral judgment about the main premise.

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

Rationale

In Rationale, an argument is like an upside-down tree, with the roots being the main contention. It is made up of simple, linked arguments that constitute the justification for affirming or denying the main contention. Each argument is a claim with a single reason supporting it or an objection to it. Each reason or objection is made up of one or more claims that work hand in hand to provide the justification for the claim above them. The main contention starts the argument and needs to be evaluated as either true or false. The contention has to be a full, grammatical, declarative sentence. It should also be normative or moral; it should make an evaluative judgment about the rightness or wrongness of the action in question.

Reasons should directly address the idea in the claim above them; that is, they should answer "why" or serve as "because" for the claim above them.[22] Reasons or objections should observe three rules: the golden rule, the rabbit rule, and the holding hands rule. The golden rule states that every argument has at least two supporting premises. This is to ensure that even obvious or hidden supporting premises are explicated. The rabbit rule states that any important term or concept that appears in the contention must also appear in one of the premises. This is to make sure that the contention is appropriately tied to the premises. The holding hands rule states that if something appears in a premise but not in the contention, it must appear in at least another premise, to make sure that the premises are tied to each other.

The Argument

The argument, presented here in text format, was developed based on the Rationale argument; the diagrammatic version is available online.[23,24] The argument proceeds as follows:

> Contention: The use of data mining by PHI companies in Australia is ethical.[25] There are three reasons for this: (1) PHI companies in Australia cannot use data mining to perform risk rating; (2) the use of data mining by PHI companies in Australia can help improve the products and services; and (3) the use of data mining by PHI companies in Australia can help with fraud detection. However, there are five objections to this line of reasoning: (1) data mining can be used by PHI companies in Australia in an unethical manner; (2) the use of data mining by PHI companies in Australia can violate customers' privacy; (3) the use of data mining by PHI companies in Australia is done without the consent of customers; (4) the use of data mining by PHI companies in Australia may involve the secondary use of data; (5) and the use of data mining by PHI companies in Australia may involve using data for unintended purposes. These reasons and their support or objections are detailed below.
>
> The use of data mining by PHI companies in Australia does not raise an ethical issue because PHI companies in Australia cannot use data mining to perform risk rating. Indeed, risk rating is illegal in Australia, as the Health Insurance Companies Act 2007 prohibits it. Data mining will not be used in this unethical manner, as the illegality of risk rating means there is no incentive to use it to risk rate customers. However, there are other incentives to perform data mining. For example, data mining can be used to detect fraud or improve the products and services. This means

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

that PHI companies in Australia can still use data mining, possibly in an unethical manner, which suggests that unless risk rating is the only possible unethical use of data mining, we cannot exclude possible unethical uses.

Data mining by PHI companies in Australia can be potentially used to help with fraud detection. Detecting fraud can reduce financial loss and protect revenue, which, in turn, can result in savings to customers. Moreover, detecting fraud can help PHI companies in Australia to remain financially sound, which is important for existing customers so PHI companies can pay their claims into the future. Similarly, the use of data mining by PHI companies in Australia can facilitate the provision of tailored products and services and help improve products and services. This can reduce PHI companies' costs and, in turn, reduce premiums for customers.

Conversely, data mining can be used by PHI companies in Australia in an unethical manner. For example, data mining can be used to classify a customer as belonging to a group that is likely to default on payments, a classification that may not be fair. What if, in reality, the customer does not belong to the group the classification assigned to him or her? This potentially devalues a customer who does not know, and so cannot correct, an inaccurate conclusion about him or her. The inability of the customers to correct their information contravenes their right to control their own data, thereby violating their privacy. Similarly, data mining can be used by PHI companies to classify a customer as belonging to a group that is likely to develop a certain disease. If this is true, a customer may not want others to know this. For this reason this classification violates the customer's privacy.

However, PHI companies in Australia are obligated to de-identify customers' data, thereby protecting against this type of breach of privacy. Furthermore, PHI companies in Australia cannot use this information to deny the customer insurance or charge him or her higher premiums.

Still, the use of data mining by PHI companies in Australia may be performed without the consent of customers. Indeed, not seeking permission from customers is unethical, as using data without customers' consent violates their human rights. Their rights to be autonomous agents, to be free (the right to liberty), to feel secure, and to be treated with respect have all been contravened. The violation of these human rights is wrong. Furthermore, the use of data mining by PHI companies in Australia may involve the secondary use of data. Secondary use of data breaches customers' right to have control over their own data. This violates their privacy and is wrong. It is worth noting that the secondary use of data is not protected by Australian privacy laws, as the laws protect only the first use of the data. This makes the secondary use of data even more problematic, prompting a need for its protection by law. A further objection to the use of data mining by PHI companies in Australia involves using data for an unintended purpose. This use of data is problematic for two reasons. First, using data for an unintended purpose could expose data to abuse, causing harm to individuals. Second, using data for an unintended purpose is against the Australian privacy laws. The IPPs specifically state that data should not be used for a purpose for which the information is not relevant. Both subjecting individuals to harm and breaching the Australian privacy laws make using data for an unintended purpose wrong.

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

The Ethical Analysis

The preceding section laid out the argument for and against the use of data mining by PHI companies in Australia. The aim of this section is to draw on classical philosophical theories such as utilitarianism, Mill's harm principle, Kant's deontological theory, and Helen Nissenbaum's contextual integrity framework to highlight the important aspects in the preceding argument about privacy. Using a philosophical perspective provides a philosophical basis for our attempt to arrive at a moral judgment about the threat data mining by PHI companies poses to privacy. However, a definition of and an overview of the value of privacy are given to provide context to the ethical analysis.

There are three standard theories of privacy: accessibility privacy defines privacy in terms of one's right to be physically left alone. Decisional privacy focuses on freedom from interference in one's choices and decisions. Informational privacy defines privacy as control over the flow of one's personal information.[26] Because this article is concerned with the use of customers' personal information by PHI companies for data mining purposes, it is this third definition that is most relevant for this article. The definition of informational privacy focuses on the customers' ability to restrict access to and maintain control over the flow of their personal information, including the transfer and exchange of that information.

Privacy is important for many reasons, including such human ends as trust, friendships, security, love and marriage relationships, respect and dignity, freedom of expression and liberty, autonomy, democracy, solitude, anonymity, secrecy, data protection, and self-confidence.[27] Privacy is also valued because it can protect individuals from such various harms as defamation, harassment, manipulation, blackmail, theft, subordination, and exclusion. James Moor[28] considers privacy as the articulation of the value of security. Privacy is also important because it affords individuals the ability to selectively disclose information relating to their self.[29] This control over and management of self-presentation is vital for individuals to be able to successfully create and maintain different kinds of personal relationships. In other words, our ability to navigate a variety of social interactions depends on our ability to control information about our self. Without privacy, the variety of relationships individuals can participate in would disintegrate. So basic is the need for privacy, it is often simply assumed to be an individual right.

According to Kant's means-to-an-end categorical imperative, it would appear that the use of data mining by PHI companies is wrong because customers were used as a means to an end—the means being the customers' personal information, and the end being such secondary goals as the detection of fraud or the improvement of products and services. Respect for people requires that customers be treated as ends in themselves, and not only as means to some other end. To treat customers with respect obliges companies to treat them as persons who have value in themselves, not just as sources of pieces of information that PHI companies could feed to a data mining application to add value to their business.

Taking a utilitarian perspective—the morally right action is that which produces the greatest good—may yield a different outcome. If using data mining in the PHI context produces considerable good, then using data mining is not wrong. It has already been found that data mining can help with detecting fraud, improving products and services, streamlining advertising, and improving companies' understanding of customer's behavior—outcomes that all appear to help PHI companies to remain financially sound. This is important for existing customers, because it means PHI companies can pay their claims into the future. In addition, given that risk rating is illegal and de-identification protects customers' privacy, it would appear data mining does little, if any, harm to their customers, suggesting that the use of this technique would be acceptable.

However, in analyzing the use of data mining using Mill's harm principle,[30] it would appear that the secondary use of customers' personal information for unintended purposes and without the consent of the customers is unfair, wrong, and illegal. Secondary use of personal information could expose data to abuse, which, in turn, could result in harm to customers. Using customers' data for unintended purposes and without the consent of the customers also violates their basic human rights and their privacy.

Helen Nissenbaum's contextual integrity framework has two types of informational norms: (1) norms of appropriateness and (2) norms of distribution.[31] *Norms of appropriateness* dictate the nature of the information about an individual that is permissible to reveal in a particular context. For example, it is proper for Mrs. X's professor to inform the dean of the college of Mrs. X's misconduct, but it is not acceptable for the professor to share this information with her husband. *Norms of distribution* govern the flow of information from one party to another—whether or not that distribution of information respects contextual norms of information flow. Using the same example, it is acceptable for Mrs. X's professor to email the dean of the college the evidence of misconduct, but it is inappropriate for the professor to email it to her friend. The contextual integrity of the flow of information is maintained when both kinds of norms are respected; otherwise, a breach of privacy occurs.

In analyzing the use of data mining by PHI companies in Australia, it would appear that the secondary use of customers' personal information by PHI companies in Australia is not appropriate, because this use is for a context other than the one for which the information was gathered. The absence of consent from the customers for their personal information to be used in other contexts makes this secondary use even more inappropriate. Although the norms of distribution have not been violated in this case, because distribution of personal information did not occur, the norms of appropriateness have been violated; thus the use of data mining by PHI companies in Australia breaches customers' privacy and is therefore wrong.

Conclusion

The aim of this article was to examine the threats to the privacy of the Australian PHI customers arising from the use of data mining. To achieve this aim, qualitative interviews with key experts and a search within Australian governmental and nongovernmental websites relevant to PHI were conducted. Using the results from these empirical approaches, the article then developed an argument to deliberate on the ethicality of the use of data mining by PHI companies. The argument was developed using Rationale, a critical thinking tool, and was followed by an ethical analysis that utilized four classical ethical theories—utilitarianism, Mill's harm principle, Kant's deontological theory, and Helen Nissenbaum's contextual integrity framework—to arrive at a moral judgment about the use of data mining by PHI companies.

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

The argument found that the use of data mining by PHI companies in Australia is unethical. It is true that the risk to the privacy of PHI customers emanating from the use of data mining is significantly reduced because Australian privacy laws prevent PHI companies from using data mining to perform risk rating and from using personal information for an unintended purpose, and also because the Australian PHI companies are obligated to de-identify customers' data before sharing them with a third party. However, there are other incentives to perform data mining on customers' data, and there are gaps in the Australian privacy laws that allow PHI companies to apply data mining applications to their customers' personal information.

Other incentives for the use of data mining are improvement of products and services, detection of fraud, and streamlining of marketing efforts. Australian privacy laws don't appear to prevent the secondary use of data. This may mean that data mining could be used by PHI companies in Australia in an unethical manner, such as to classify a customer as belonging to a group of customers who are likely to default on payments or are likely to develop a certain disease. Both of these scenarios entail a threat to the customers' privacy, even if PHI companies can't use this information to discriminate against the customer. The use of data mining by PHI companies in Australia is also wrong because it is done without the consent of customers, which violates the customers' basic human rights.

The results of the philosophical analysis appear to back up the contention of the argument. Although the utilitarianism perspective supported the view that data mining in PHI may not be wrong, because it can produce considerable good in comparison to the adverse effects, applying the three other theories yielded a different conclusion. The secondary use and the absence of consent violated both Kant's means-to-an-end categorical imperative and Helen Nissenbaum's contextual integrity norms of appropriateness. The secondary use of customers' data is also wrong according to Mill's harm principle, because it could expose data to abuse, which in turn could result in harm to customers. It is also a violation of customers' human rights, given that it is done without their consent.

In the United States, PHI companies are known to use data mining to cherry-pick their customers,[32] and it is mainly for this reason that data mining in the context of PHI is an area of major privacy concern. Although the situation in Australia differs from that in the United States, in that data mining cannot be used to perform risk rating and personal information cannot be used for unintended purposes because these actions are illegal in Australia, data mining can still be used in Australia to violate customers' privacy. This suggests that the concerns raised in the predominately American literature about data mining are still valid. It also suggests that although the privacy laws in Australia are slightly tighter compared to those in the United States, the situation with regard to the use of data mining is not much better.

To improve the situation in Australia, the Office of the Australian Information Commissioner (OAIC), as the independent privacy regulator, may want to consider adding a governing system to its current operations. This will not only make monitoring of compliance with the privacy laws more effective but will also limit the capacity of data mining to be used for violating customers' privacy. Thus, in addition to conducting annual audits and investigating complaints from the general public, which the OAIC currently does, or instead of leaving it, in this case, to the health insurance companies to self-regulate the behavior of their employees,

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

the OAIC could take a more proactive approach by introducing a governing system that specifically monitors the use of data mining within the health insurance sector.

Putting restrictions, possibly in the form of laws and regulations, on the use of data mining by health insurance companies can also help reduce the harm that may be inflicted on customers and protect their basic human rights and their privacy. Thus, whereas data mining can be used to cause harm to customers or can violate their privacy or basic human rights, protecting privacy through laws can protect customers from such harms and violations.

Notes

1. Tavani HT. Ethics and technology: Controversies, questions, and strategies for ethical computing. 4th ed. Hoboken, NJ: John Wiley; 2013.
2. Borna S, Avila S. Genetic information: Consumers' right to privacy versus insurance companies' right to know a public opinion survey. *Journal of Business Ethics* 1999;19:355–62.
3. Danna A, Gandy O. All that glitters is not gold: Digging beneath the surface of data mining. *Journal of Business Ethics* 40;2002:373–86.
4. Angst CM. Protect my privacy or support the common good? Ethical questions about electronic health information exchanges. *Journal of Business Ethics* 2009;90:169–78.
5. Raychaudhuri K, Ray P. Privacy challenges in the use of eHealth systems for public health management. *International Journal of E-Health and Medical Communications* 2010;1(2):12–23.
6. Al-Saggaf Y, Islam Z. A malicious use of a clustering algorithm to threaten the privacy of a social networking site user. *World Journal of Computer Application and Technology* 2013;1(2):29–34.
7. Al-Saggaf Y. The mining of data retrieved from the eHealth record system should be governed. *Information Age* 2012 Nov/Dec:46–7.
8. Sarathy R, Robertson CJ. Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics* 2003;46(2):111–26.
9. Van Wel L, Royakkers L. Ethical issues in web data mining. *Ethics and Information Technology* 2004;6:129–40.
10. See note 5, Raychaudhuri, Ray 2010.
11. Yoo I, Alafaireet P, Marinov M, Pena-Hernandez K, Gopidi R, Chang J, et al. (2012). Data mining in healthcare and biomedicine: A survey of the literature. *Journal of Medical Systems* 2012;36:2431–48.
12. See note 4, Angst 2009.
13. See note 2, Borna, Avila 1999.
14. See note 9, van Wel, Royakkers 2004.
15. Hildebrandt M. Who is profiling who? Invisible visibility. In: Gutwirth S, Poullet Y, de Hert P, de Terwangne C, Nouwt S, eds. *Reinventing Data Protection?* Berlin: Springer; 2009: 239–52.
16. Willison DJ, Keshavjee K, Nair K, Goldsmith C, Holbrook AM. Patients' consent preferences for research uses of information in electronic medical records: Interview and survey data. *British Medical Journal* 2003 Feb 15:326–73.
17. See note 1, Tavani 2013.
18. http://phiac.gov.au (last accessed 3 Aug 2014).
19. privatehealth.gov.au (last accessed 3 Aug 2014).
20. http://www.comlaw.gov.au/Details/C2012C00590 (last accessed 3 Aug 2014).
21. Twardy C. Argument maps improve critical thinking. *Teaching Philosophy* 2004;27(2):95–116.
22. Rationale. *Learn*. Austhink; 2012; available at http://rationale.austhink.com/learn (last accessed 14 Aug 2014).
23. http://csusap.csu.edu.au/~yalsagga/RationaleArgument.gif (last accessed 14 Aug 2014).
24. It is important to note that this argument draws its information from the results of the qualitative interviews, the search of the governmental and nongovernmental websites, and the literature. It is beyond the scope of this article to offer a fully fleshed argument.
25. This is the main contention of the argument.
26. See note 1, Tavani 2013.
27. Al-Saggaf Y, Islam Z. Privacy in social network sites (SNS): The threats from data mining. *Ethical Space: The International Journal of Communication Ethics* 2012;9(4):32–40.
28. Moor J. Towards a theory of privacy in the information age. *Computers and Society* 1997;27:27–32.

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press

29. Rachels J. Why privacy is important. *Philosophy & Public Affairs* 1975;4:323–33.
30. Mill JS. *On Liberty: Annotated Text, Sources and Background Criticism*. New York: W.W. Norton; 1975 [1859].
31. Sar RK, Al-Saggaf Y. Contextual integrity's decision heuristic and social network sites tracking. *Ethics and Information Technology* 2013;15(4):1–12.
32. See note 2, Borna, Avila 1999. See note 3, Danna, Gandy 2002. See note 4, Angst 2009.

https://doi.org/10.1017/S0963180114000607 Published online by Cambridge University Press