Journal of Media Ethics, 30:19–30, 2015
Copyright © Taylor & Francis Group, LLC
ISSN: 2373-6992 print/2373-700X online
DOI: 10.1080/08900523.2014.985297

The Good, the Bad, and the Ugly: Applying Rawlsian Ethics in Data Mining Marketing

Stephen Cory Robinson
Department of Journalism and Media Communication, Colorado State University

Using a Rawlsian approach to analyze the ethical implications of data mining within three major codes of ethics used by American marketing firms, the author argues that marketers should re-conceptualize their business conduct, as defined in their individual codes of ethics, to incorporate a Rawlsian concern for society's least advantaged members. Rawls's concept of primary goods provides the framework for the argument that anonymity, a component of privacy, is vital for consumers whose autonomy is affected by data mining. A combination of practical measures, ethical guidelines, and legislative protections are recommended for minimizing concerns about data mining, while still allowing for commercial advantages provided by the practice.

"*Computers have promised us a fountain of wisdom but delivered a flood of data.*" (Frawley, Piatetsky-Shapiro, & Matheus, 1992, p. 57)

INTRODUCTION

The Internet is an innovative, interactive medium where individuals can search for and locate information, socialize with friends and family, and even purchase goods and services. In 2013, more than 2.7 billion individuals use the Internet (International Telecommunication Union, 2013). Any individual can inadvertently divulge information (including private information such as name, age, date of birth, and product preferences) on a website that can then be collected, stored, and used by that website. Thus, despite its usefulness, widespread Internet use also leads to a variety of new questions regarding individual privacy and the commercial use of personal information. New technologies thus introduce a number of ethical and personal safety concerns that will have to be addressed as we move forward in the technological age.

Manuscript submitted June 30, 2014; revision accepted October 14, 2014.

Correspondence should be sent to Stephen Cory Robinson, Department of Journalism and Media Communication, Colorado State University, 1785 Campus Delivery, Fort Collins, CO 80524. E-mail: cory.robinson@colostate.edu

Recently, consumer advocates have raised concerns that personal information collected from individuals during their Internet sessions may be used without the consumer's knowledge. When consumers utilize digital personal assistant Siri on their Apple iPhone, for instance, their information is collected and sent to Apple's servers. This personal information is associated with an anonymous number for six months and then kept for an additional 18 months for product testing and improvement (McMillan, 2013). Moreover, companies such as eBay and MasterCard now share consumer information with marketers in an attempt to increase digital advertising and marketing (Green, 2013; Kaye, 2013). These examples point to an increasingly serious problem in Internet usage, where personal information knowingly shared on one site may flow through a variety of additional electronic channels without the express permission or knowledge of the individuals whose information is aggregated and utilized.

In this article I define the current data-collection practices known as *data mining*, analyzing both its positive and negative ramifications. In considering the ethical implications of data mining, in particular, I argue that marketers should re-conceptualize their ethical obligations of business conduct to incorporate a Rawlsian concern for the individual. Rawls grants a high level of importance to protecting the individual, suggesting that anonymity and privacy be built into information exchanges (Rawls, 1999). In addition, I will outline several implications for marketers and advertisers regarding the proposed changes to current data-mining practices.

DATA MINING

Data Mining Defined

Data mining is a set of methodologies for extracting knowledge from data sets (IBM, 2013). These methodologies allow firms to use data from specific data sets to develop and initiate complex relationship-management strategies (Danna & Gandy, 2002). In addition to the collection of information from databases, as in data mining, the aggregation of data can also take place on the World Wide Web. This practice is defined as *web mining*, or the use of data-mining techniques applied to the web (Cooley, Mobasher, & Srivastava, 1997). It should be noted, therefore, that the concept of data mining is quite complex, composed of multiple online and offline data-gathering practices.

The concept of data mining can best be characterized as "the process of extracting or detecting hidden patterns of information from large databases" (Ngai, Xiu, & Chau, 2009, p. 2593). Data mining allows aggregate gathering of information (Chung & Grimes, 2006), often using a plethora of tools to collect information from various offline and online activities (Danna & Gandy, 2002). Through data mining, detailed behavioral and demographic profiles of users can be created (Craig, 2011). Collecting aggregate data, rather than gathering individuals' personal information, allows marketers to assess user interest and patterns of Internet usage in order to determine a user's likes, dislikes, patterns of purchases, and the like (Chung & Grimes). A common example of data mining is the collection of data concerning Internet users' online media viewing. For instance, both Amazon and Netflix use data-mining systems to compile viewer recommendations based on their choices of previously viewed media (Nissenbaum, 2009). Although such uses of information may seem at first glance to be pro-consumer, the personal nature of these services is based on specific uses of personal information that may or may not be kept private by companies. Targeted advertising is a common result of tracking user purchases as well as media preferences, and these data analyses tend to be quite accurate.

Advantages of Data Mining

Because businesses are one of the main stakeholders in data mining (Payne & Trumbach, 2009), they stand to reap a number of benefits from utilizing data-mining information. A major business advantage of data mining is that it increases the ability of marketers to discover and predict who their most profitable customers will be (Danna & Gandy, 2002). Agencies are also able to increase consumer satisfaction by using data-mining techniques (Payne & Trumbach). By noting and applying consumer preferences for channel of communication (such as social media, email, phone) and time of day for contact, marketers can integrate consumer preferences into their customer-contact strategies. Companies and organizations also use data mining to target products to specific consumers. By drawing upon their familiarity with an individual's purchasing behaviors and product-search inquiries, businesses can provide a customer with a more targeted and desired product or service (Olson, 2008). Additionally, businesses can utilize profile data to build products that are theoretically of "higher value" for customers (Olson, p. 5). Finally, these techniques also enable marketers to broaden consumer exposure to products, while simultaneously decreasing marketing costs (Olson). While it would be naive to argue that people should avoid using the Internet because data-mining practices like targeted marketing can pose threats to their privacy, there are too few controls and protections in the current environment to ensure that personal data are not misused by marketers. I argue that greater built-in privacy protection for Internet, particularly if the movement to ensure privacy is led by the marketers themselves, will in the end strengthen the Internet realm for users and marketers alike.

Businesses are not the only entity to gain from data mining: Consumers can also benefit from advance notification of sales or discounts for their allegiance to a certain brand (Payne & Trumbach, 2009). These various benefits may equate to helping the consumer save both time and money (Payne & Trumbach). Yet, again, the issue of privacy and control over one's own personal information rears its ugly head, even when this information is ostensibly used to offer consumers perks and save them money. As the Internet develops, built-in consumer privacy protections can benefit marketers and consumers alike, making consumers more confident that their information will not be widely shared and actually increasing the likelihood that people will buy online. Without such protections, more and more consumers may simply abandon ship, and the advantages of the Internet could easily give way before its disadvantages, particularly those inherent in data mining.

Disadvantages of Data Mining

Despite the significant corporate advantages inherent in the use of data mining techniques by marketers, social and legal concerns about their widespread use abound. Not only are privacy issues of great concern because of burgeoning Internet scams that range from identity theft to work-at-home schemes that turn out to be rip-offs (Olson, 2008; Ngai et al., 2009). Due to the sheer amount of information that can be collected through data mining, in addition to its relatively open availability on the Internet, we have seen that consumers often lack control over what happens to their data (Payne & Trumbach, 2009). By agreeing to a website's term-of-use contracts, users may unknowingly be authorizing their personal information and web interactions (including responses and submissions) to become the exclusive property of the website (Chung & Grimes, 2006). When unwary consumers relinquish their right to ownership of personal information to a website, a number of ethical issues may arise.

Analyzing such ethical concerns about ownership of digital content, Lyon identifies the concept of "social sorting" (Lyon, 2002a). Social sorting, the coding and classifying of aggregate data, affects and influences both the choices and opportunities of profiled individuals (Lyon, 2002b). Through social sorting, customers can be classified according to specific demographic variables, including current net worth (Lyon, 2002b), which may affect not only their privacy, but also their access to credit and goods. Currently, there are few protections for information collected and stored in aggregate data (Chung & Grimes, 2006), and "laws do not clearly define the restrictions that companies have based on what they say in their privacy policies" (Payne & Trumbach, 2009, p. 243).

Chung and Grimes (2006) posit three ethical concerns stemming from the use of data mining: price discrimination, "weblining," and access to personal information in the public sphere. Through the use of collected data, companies can segment and sort consumers, even at times classifying consumers by their income (Danna & Gandy, 2002). By segmenting customers according to their income, marketers could presumably even begin to price and offer products to individuals based on their presumed purchasing power, rather than offering a single price point to all consumers. Additionally, consumers can experience weblining, the practice of denying someone access and service based on their online presence (Danna & Gandy). Consumers with an undesirable profile may not be offered the same goods and services as consumers who fit a profile deemed more desirable by a marketer or organization (Andrews, 2012). Additional concerns related to data mining include the increased potential for identity theft, as consumers willingly disclose personal information in order to gain access to member loyalty cards and other benefits. Customers may even be compelled to divulge personal information as a prerequisite for eligibility to make purchases from specific companies, such as Sam's Club or Costco (Payne & Trumbach, 2009). As we read and hear about on a daily basis, such Internet business practices can leave consumers open to various scams, and this situation is bound to worsen if controls are not put into place to govern the uses of consumer information.

Technological Determinism

In analyzing data mining and its role in the life of technology users, it is beneficial to consider the effect of technological determinism. *Technological determinism* is the belief that advances in technology, more than any other factor, are what push social change (Smith & Marx, 1994). It is true that advances in technology (such as the printing press or personal computer) influence and change cultural values and societal norms. For example, with the development of the smartphone, and its intrusion into private life, what is considered appropriate behavior in public spaces has now changed. If, in the past, phone calls were considered quite personal, we know that today hearing a personal phone call at the grocery store or on campus is par for the course. Additionally, using a cellphone while dining at a restaurant used to be considered taboo, but it is quite common now, even in the presence of a spouse or partner.

In contrast to technological determinism, the theory of *social determinism* holds that society drives changes in technology (Herschel & Andrews, 1997; Peace, Weber, Hartzel, & Nightingale, 2002). Rather than technology being inherently value-laden, technology is value neutral. Supporting the view of technological determinism, then, data mining is a technology that shapes society and is value-laden. Rather than being value-neutral, data mining technologies have one main purpose: to vacuum up and sort as much personal information as the technology can acquire.

For example, the Amazon customer who desires a book recommendation based on previous purchases is easily provided with suggestions through Amazon's advanced algorithms. While this information provided in a product review seems simple on its face, the style of the writing can lead to the identification of the reviewer, and in turn, tracking of the individual reviewer's movements through the Internet (Afroz, Islam, Stolerman, Greenstadt, & McCoy, 2014). Many consumers do not balance the growing risks of information sharing (i.e., identify theft, phishing schemes, discrimination) with the convenience provided by advanced consumer services of this type. Through technological determinism, online marketing technologies, including data mining, are changing purchasing and online browsing behaviors, as well as social norms and rules, encouraging consumers to divulge important personal information for potentially trivial gains, risking identity theft, mail fraud, and even public exposure in order to more easily locate interesting media sources or a preferred style of clothing. While data mining resulting in product and service recommendations may make shopping, media viewing, and information gathering easier for the consumer (Payne & Trumbach, 2009), consumers also sacrifice anonymity, privacy, and autonomy when they divulge their personal information online (Kang, Brown, & Kiesler, 2013; Rainie et al., 2013).

THEORETICAL FRAMEWORK

Rawlsian Ethics Overview

Rawls's *A Theory of Justice* (1971) incorporates two main principles: the *Equal Liberty Principle* (each person has equal access to basic liberties) and the *Difference Principle*, which maintains that social and economic inequalities should be arranged so as to be of greatest benefit to the least advantaged in society (Rawls, 2001). The application of Rawls' ethical approach places the majority of emphasis in business on the protection of the individual (2001).

As described in Rawls's difference principle, the least advantaged in society are of particular concern when analyzing the social effects of data mining practices. Specifically, how might social and economic inequalities be structured or enacted so that the greatest benefits of current technologies are available to the least advantaged? Additionally, Rawls (2001) makes a provocative statement about the least advantaged in society: "In a well-ordered society, all citizens' equal basic rights and liberties and fair opportunities are secure, the least advantaged are those belonging to the income class with the lowest expectations" (p. 59).

I argue that individuals without Internet access or proper media literacy should be considered as among the least advantaged. This assertion leads to a number of important questions, since, if we are to form a well-ordered technological society, it would seem that respect for the rights of lower-income individuals needs to be built into Internet marketing practices from the outset. Yet how secure are the basic rights of such lower income people today within the newest forms of consumer data gathering and marketing techniques using advanced technologies? More importantly, should the existing economic disadvantages of the "least advantaged" simply be recreated on the Internet through current technological practices that serve to exclude certain groups while propagating the relative advantages of others?

Critical to the concept of the least advantaged is Rawls' (2001) definition of *primary goods* as "what free and equal persons need as citizens" (p. 60). As such, I argue that the Internet has become so pervasive and necessary in everyday life (i.e., shopping, education, news, media consumption), that the Internet itself can now be seen as a primary good. As a minimum, broadband Internet should be seen as a primary good, as it is the lowest tier recommended for Internet access by many government groups, including the U.S. Federal Communications Commission (2010) and the United Nations (2011). In addition to being a primary good, Internet access should be considered a basic human right. *Human rights* are inherent to human beings, and all human beings are equally entitled to these rights without suffering discrimination (United Nations, 2014), and these rights should include Internet access. On its Human Rights for Internet Users website, the Council of Europe (2014) states that citizens have a right to Internet access because it allows them to exercise their rights and freedoms to participate in democracy. In Estonia, Internet access has been a basic human right since 2000 (Woodward, 2003), and other nations have since adopted this policy. Bolstering this argument, Mathiesen (2014) recently noted that Internet access is a human right allowing for access to seeking and receiving information. Through the Internet, individuals are able to communicate, deliberate with others, and be informed (Mathiesen). Yet many of the so-called least advantaged citizens of the world now lack even basic Internet access. Without Internet access, how can the least advantaged keep up with their more technologically savvy and involved fellow citizens?

Privacy, too, can be seen as a primary good as it allows for anonymity and other crucial principles related to self-development. Privacy as a primary good should include the concept of anonymous existence online, or "the state of being not identifiable . . . " (Pfitzmann & Köhntopp, 2001). Rawls's (2001) concept of primary goods states that scarcity is a concern regarding these goods, since the availability of unlimited goods would allow each individual to simply acquire all he or she desired (Plaisance, 2009). Anonymity, as a primary good, should be treated as scarce and should have value in the online realm. Without anonymity, identification of individuals can occur, which may ultimately lead to discrimination based on these identifiers. Consequently, the least advantaged should be among the main considerations when respecting this primary good of anonymity. By protecting the least advantaged, these individuals are able, through anonymity, to have a private existence, and not suffer social sorting, web lining, or other forms of discrimination. Anonymity becomes a form of self-protection and self-development for all Internet users, and more importantly for the least advantaged.

Anonymity as a primary good is thus a vital element in creating and maintaining privacy. The concept of anonymity actually assumes the right to privacy, including maintenance of social relations and development of the self (Plaisance, 2009). Development of self is crucial for individuals. Only through the right to privacy are individuals able to achieve full personhood (Plaisance). Since "privacy may also be a vehicle through which individuals construct a healthy sense of self and come to view themselves as autonomous beings" (Byford, 1998, p. 7), privacy contributes to the very notion and existence of a self. Additionally, the possession of anonymity and privacy allow individuals to maintain and control their social relations because concealing things from the public can hinder social breakdowns (Schoeman, 1992). Further, by serving multiple social roles through making choices about concealing and revealing information, thoughts, and actions, individuals are able to maintain social relationships (Nagel, 2002).

If Rawls's (1997) theory of distributive justice and the protection of the least advantaged are legitimate concerns, how do current marketing organizations, through their codes of conduct, enact protective measures for these individuals, ensuring the treatment of anonymity as a primary good? The following sections examine the codes of ethics of three major American marketing organizations, exploring how, or whether, each organization provides access for protection of the least advantaged through the protection of anonymity.

APPLICATION OF THEORY

Major American Marketing Associations

In a recent web search (January 27, 2014) of the search term "*marketing associations*," the top 10 search results across Yahoo, Google, and Bing consistently included the American Marketing Association (AMA), the Business Marketing Association (BMA), and the Direct Marketing Association (DMA). Because of the marketing firms' pervasive Internet presence, I will analyze each code of ethics in terms of Rawls's (2001) concepts of social primary goods. I look specifically at anonymity and at how each organization does or does not provide mechanisms to protect the anonymity of the least advantaged.

American Marketing Association's Code of Ethics

In the AMA code of ethics, marketers are instructed to "Do no harm" (American Marketing Association, 2013, para. 2) by consciously avoiding harmful actions. The code of ethics also explains the role of concepts such as honesty, responsibility, fairness, respect, transparency, and citizenship. The AMA (2013) defines its corporate responsibility as the attempt to "avoid using coercion" (p. 2), while simultaneously recognizing the company's special commitment to "vulnerable market segments" and "others who may be substantially disadvantaged" (p. 2). The code of ethics in this section specifically addresses the needs of the least advantaged, with the AMA (2013) defining "vulnerable market segments" (p. 2) as children, seniors, and the "economically impoverished" (p. 2). The AMA thus acknowledges both the existence of least advantaged groups and accepts at least some responsibility for protecting them.

The AMA also acknowledges the concept of anonymity in the "Fairness" section, which states that the company will "seek to protect the private information of customers, employees, and partners" (p. 2). Unfortunately, this is the only reference to the protection of anonymity in this code of ethics. While no direct mention of anonymity is made in the code, its language seems to assert, at least on face value, that the AMA is interested in protecting the least advantaged. "Harm" (p. 1), "foster trust" (p. 1), and "embrace ethics" (p. 1) are a few examples of the protection-related vocabulary appearing in the introductory page. This vocabulary sets the tone for how the AMA appears to perceive its customers and stakeholders. The AMA also recommends "avoiding the use of coercion" (p. 2). The organization rejects manipulation and other sales tactics that "harm customer trust" (p. 2). A spirit of equality and treating all stakeholders equally is even more present in the notion that AMA recommends treating "everyone, including our competitors, as we would wish to be treated" (p. 3).

Business Marketing Association's Code of Ethics

The BMA's (2013) code primarily addresses anonymity by stating that marketing activities should be targeted rather than indiscriminate. The code recommends that individuals be allowed choice in either opting in or opting out of promotions (including emails and telemarketing). Importantly, the code also states that marketers should avoid "the use of names gathered by surreptitious methods" (p. 1). Thus the BMA is less specific about the role and importance of anonymity in ethical codes than the AMA.

On the other hand, the BMA's code is similar to the AMA code in that the BMA's code (2013) utilizes words and phrases that refer to those unable to protect themselves: the least advantaged. The BMA's ethical code is rife with protection-related phrases and words, including "equal access" (p. 1), "fairly and consistently" (p. 1), "shall not ... obtain preferred status" (p. 1), or "unfairly disparage" (p. 1). The document also highlights that all "distributors or other channel partners shall be given equal access" (p. 1) with regard to promotions and assistance; apparently, the BMA does not apply protection for the least advantaged, but instead allows all organizations equal access to the least advantaged. However, the BMA does provide clear, coherent principles for how marketers must protect their customers' information. Yet there remains a marked lack of content dealing specifically with how to increase fairness toward less advantaged groups.

The BMA's code of ethics presents a clear set of protection guidelines, but they appear to set a minimal level of protections, whereas the AMA appears to embrace more fully the Rawlsian notion of the least advantaged, outlining at least in part how to protect these individuals. In contrast to the protection of the least advantaged and more consumer-oriented code of ethics of the AMA, the BMA's code of ethics addresses more marketer and organization related principles, lacking not only built-in protections for the least advantaged but also for the primary good of anonymity.

Direct Marketing Association's Code of Ethics

The DMA's (2011) code of ethics addresses marketing to children, different forms of promotions (i.e., sweepstakes and special offers), and different forms of marketing (i.e., digital, mobile, and telephone). While the document revealed no occurrences of the term "anonymity," the DMA code of ethics does present a six-page section detailing the "collection, use, and maintenance of marketing data" (Direct Marketing Association, 2011, p. 18). The DMA code presents market-focused guidelines for the solicitation of individuals and the collection and handling of personal information. While the DMA is thorough in the specific areas addressed, there are no specific mentions of harm, equality, trust, or related concepts. The DMA code functions as a "how to" for marketers seeking to comply with ethical solicitation and data collection practices. Because consumers, marketing organizations, and government are the stakeholders most affected by data mining (Payne & Trumbach, 2009), the DMA sorely needs to address consumer issues, in particular by better defining who is most likely to be harmed by the practices.

After examining each of the three codes of ethics, it is evident that each one incorporates some degree of Rawlsian principles. References to anonymity, vulnerable market segments, fairness, and respect all speak to values and principles championed by Rawls. Rather than making bold, clear, and effective statements of these principles and values, however, these marketing associations typically allude to them without mentioning them directly.

IMPLICATIONS

Recommendations for Updating/Revising Codes of Ethics

Despite the depth of the three codes of ethics, there is a clear need in today's environment to update and revise ethical codes that pertain to the Internet and data mining. One of the biggest hurdles to enacting consumer protections on the Internet is determining who owns an individual's personal information online, including online interactions (responses, submissions, and so forth), browsing history, and personally produced digital content (videos and images, for example). Digital ownership should be more clearly and concisely defined in all three codes of ethics. Such definitions could then serve as guidelines for individuals and companies alike in making decisions about how and when personal data are used. A more clearly stated and open ethical statement on the part of the trade groups could also point the way for individuals who are trying to figure out how to opt out of data-collection practices, helping them to make informed decisions based on clear policies that would set limits on the uses of their personal information. In addition to simplifying and correcting internal codes of ethics, companies should provide individuals with information about precisely how their personal data are being used, which will allow them the freedom either to negotiate or resist these uses of their personal information (Chung & Grimes, 2006). Only through strong digital ownership policies can individuals utilize the full potential of the Internet and information technologies without the fear of tracking and incurring other risks associated with long-term personal data collection.

To help develop the primary good of anonymity, marketers should provide and implement technologies that encourage and strengthen anonymity; for example, the Do Not Track initiative, access to Virtual Private Networks (VPN), clear opt-out and data deletion opportunities, as well as blocking technologies, including cookie blockers. Through the use of encrypted traffic, as seen in VPNs, programs that block cookies, or enabling a browser's "Do Not Track" option (opt-out settings that notify websites that third parties may not track you), and other technologies, individuals can utilize the Internet without being tracked in the way that cookies enable. Complete anonymity may not be possible online, but these technologies allow users greater control over what personal information they are voluntarily or unknowingly divulging.

Providing opportunities for individuals to comprehend and use these technologies will strengthen consumer online media literacy and allow them to fully embrace and enjoy benefits associated with anonymity. I further recommend that consumer organizations (e.g., Electronic Frontier Foundation and similar organizations) continue to provide such technology resources, along with clear instructions for implementation. Because these technologies have not yet reached critical mass, greater anonymity will not be reached unless consumers understand and properly use these technologies.

Being able to control the use of our personal data is critical, as Chung and Grimes (2006) argue. Control of one's personal data allows individuals to make decisions about disclosure, and whether or not they allow marketers to have use of potentially sensitive information. Individuals should have the right to decide how their information is extracted from their digital activities online. Due to risks inherent in disclosing personal information online, including identify theft, and fraudulent credit card charges, consumers should have complete control over their data, including when they are allowed to be collected, who can collect them, and how they can be shared. While that level of control may be difficult to achieve, individuals and the websites they interact with at least need to find the means to abide by formal and mutually understood agreements concerning the collection, storage, and use of an individual's personal information.

Marketers should ensure that information collected from individuals is "anonymized," and that it is impossible for personal information to be reversed, that is, engineered with the original discloser being identifiable (Ohm, 2010). Marketing organizations and media companies should tighten access to personal information, especially access on Facebook and Twitter through their application programming interfaces (APIs), as information obtained through data mining can be leaked through these APIs (Huxing, Gang, Kingsum, Zhidong, & Xuezhi, 2011). If hackers gain access to APIs and exploit holes in the API, users' sensitive personal data may be compromised. A scenario made possible by compromised APIs includes users being eavesdropped on by hackers accessing their laptop's microphone (Tobias, 2014).

In order to circumvent government intervention, marketers and consumers must converse about data mining and come to some agreement about the practices and how information can be used without violating consumer rights. "It is in the industry's best interest to address and remedy privacy concerns via self-regulation before the current state of activities leads to increases in government regulation" (Miyazaki, Stanaland, & Lwin, 2009). Without better and more consistent industry standards, current public concerns over the marketing practices of data mining, and the related concept of privacy, could potentially lead to new government regulations. Codes of ethics that clearly address these concerns would benefit everyone—governments, marketers, and consumers alike.

CONCLUSION

Because technology is in an ever-changing state, it is not always possible to develop ethical guidelines comprehensive enough to deal with every misuse of technology (van Wel & Royakkers, 2004). A combination of practical measures (i.e., consumers being careful who they provide information to), ethical guidelines, and legislative protections (specifically for protection of consumer personal information) are recommended for minimizing concerns about data mining, while still allowing for the advantages it provides (better targeted products, lower marketing costs, increased consumer satisfaction). By supporting anonymity and protecting the least advantaged, marketing organizations can better fulfill their ethical duty to society, and in turn, create the greatest benefit for all stakeholders.

REFERENCES

Afroz, S., Islam, A. C., Stolerman, A., Greenstadt, R., & McCoy, D. (2014). *Doppelgänger finder: Taking stylometry to the underground.* Paper presented at the 2014 IEEE Symposium on Security and Privacy, San Jose, CA. doi: 10.1109/SP.2014.21

American Marketing Association. (2013). Statement of ethics: American Marketing Association. Retrieved from http://www.marketingpower.com/aboutama/pages/statement of ethics.aspx

Andrews, L. (2012). Facebook is using you. *The New York Times.* Retrieved from http://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html?pagewanted=all&_r=0

Business Marketing Association. (2013). BMA code of ethics: Business Marketing Association. Retrieved from http://www.marketing.org/i4a/pages/index.cfm?pageid=3286-.UV3EQr_8994

Byford, K. S. (1998). Privacy in cyberspace: Constructing a model of privacy for the electronic communications environment. *Rutgers Computer and Technology Law Journal, 24*, 1–48.

Chung, G., & Grimes, S. M. (2006). Data mining the kids: Surveillance and market research strategies in children's online games. *Canadian Journal of Communication, 30*(4), 527–548.

Cooley, R., Mobasher, B., & Srivastava, J. (1997). *Web mining: Information and pattern discovery on the World Wide Web*. Proceedings from the Ninth IIEEE International Conference on Tools with Artificial Intelligence '97, Newport Beach, CA. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=632303&tag=1

Council of Europe. (2014). Human rights for Internet users. Retrieved from http://www.coe.int/web/internet-users-rights/guide;jsessionid=7422E8871EF6692B7AEB0B8AFC29997E

Craig, T. (2011). *Privacy and big data.* Sebastopol, CA: O'Reilly.

Danna, A., & Gandy, O. H. (2002). All that glitters is not gold: Digging beneath the surface of data mining. *Journal of Business Ethics, 40*(4), 373–386. doi:10.1023/A:1020845814009

Direct Marketing Association. (2011). Guidelines for ethical business practices. Retrieved from http://www.dmaresponsibility.org/Guidelines/

Frawley, W. J., Piatetsky-Shapiro, G., & Matheus, C. J. (1992). Knowledge discovery in databases: An overview. *Artificial Intelligence Magazine, 13*(3), 57–70.

Federal Communications Commission. (2010). *Sixth broadband deployment report.* Washington, DC: Author. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-129A1_Rcd.pdf

Green, D. (2013). eBay is now sharing its customer data with marketers. *Business Insider.* Retrieved from http://www.businessinsider.com/ebay-now-sharing-data-with-marketers-2013-4

Herschel, R. T., & Andrews, P. H. (1997). Ethical implications of technological advances on business communication. *Journal of Business Communication*, *34*(2), 160–170. doi:10.1177/002194369703400203

Huxing, Z., Gang, W., Kingsum, C., Zhidong, Y., & Xuezhi, X. (2011). *Detecting resource leaks through dynamical mining of resource usage patterns*. Proceedings from Forty-First International IEEE/IFIP Conference on Dependable Systems and Networks 2011, Hong Kong, China. Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5958824 doi:10.1109/DSNW.2011.5958824

IBM. (2013). Knowledge discovery and data mining. Retrieved from http://researcher.watson.ibm.com/researcher/view_pic.php?id=144

International Telecommunication Union. (2013). The World in 2013: ICT facts and figures. Retrieved from http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Kang, R., Brown, S., & Kiesler, S. (2013). *Why do people seek anonymity on the Internet?: Informing policy and design.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Retrieved from http://www.cs.cmu.edu/∼kiesler/publications/2013/why-people-seek-anonymity-internet-policy-design.pdf. doi: 10.1145/2470654.2481368

Kaye, K. (2013). Mastercard, AmEx quietly feed data to advertisers. Retrieved from http://adage.com/article/dataworks/mastercard-amex-feed-data-marketers/240800/?utm_source=update&utm_medium=newsletter&utm_campaign=adage&ttl=1366668133

Lyon, D. (2002a). Everyday surveillance: Personal data and social classifications. *Information, Communication & Society*, *5*(2), 242–257. doi:10.1080/13691180210130806

Lyon, D. (2002b). Surveillance in cyberspace: The Internet, personal data and social control. *Queen's Quarterly, 109*(3), 345–356.

Mathiesen, K. (2014). Human rights for the digital age. *Journal of Mass Media Ethics*, *29*(1), 2–18. doi:10.1080/08900523.2014.863124

McMillan, R. (2013). Apple finally reveals how long Siri keeps your data. Retrieved from http://www.wired.com/wiredenterprise/2013/04/siri-two-years/

Miyazaki, A. D., Stanaland, A. J. S., & Lwin, M. O. (2009). Self-regulatory safeguards and the online privacy of preteen children. *Journal of Advertising*, *38*(4), 79–91. doi:10.2753/JOA0091-3367380406

Nagel, T. (2002). *Concealment and exposure: And other essays*. Oxford, England: Oxford University Press.

Ngai, E. W. T., Xiu, L., & Chau, D. C. K. (2009). Application of data mining techniques in customer relationship management: A literature review and classification. *Expert Systems with Applications, 36*(2), 2592–2602. doi:10.1016/j.eswa.2008.02.021

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life.* Palo Alto, CA: Stanford University Press.

Ohm, P. (2010). Broken promises of privacy: Responding to the suprising failure of anonymization. *UCLA Law Review, 57*, 1701–1777.

Olson, D. L. (2008). Ethical aspects of web log data mining. *International Journal of Information Technology Management*, *7*(2), 190–200. doi:10.1504/IJITM.2008.016605

Payne, D., & Trumbach, C. C. (2009). Data mining: Proprietary rights, people and proposals. *Business Ethics: A European Review, 18*(3), 241–252. doi:10.1111/j.1467-8608.2009.01560.x

Peace, A. G., Weber, J., Hartzel, K. S., & Nightingale, J. (2002). Ethical issues in ebusiness: A proposal for creating the ebusiness principles. *Business and Society Review*, *107*(1), 41–60. doi:10.1111/0045-3609.00126

Pfitzmann, A., & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity: A proposal for terminology. In H. Federrath (Ed.), *Designing privacy enhancing technologies* (pp. 1–9). Berlin, Germany: Springer.

Plaisance, P. L. (2009). *Media ethics: Key principles for responsible practice.* Los Angeles, CA: Sage.

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. *Pew Research Center*. Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

Rawls, J. (1971). *A theory of justice.* Cambridge, MA: Belknap Press.

Rawls, J. (1997). The idea of public reason revisited. *The University of Chicago Law Review*, *64*(3), 765–807. doi:10.2307/1600311

Rawls, J. (1999). *A theory of justice* (rev. ed.). Cambridge, MA: Belknap Press.

Rawls, J. (2001). *Justice as fairness: A restatement.* Cambridge, MA: Harvard University Press.

Schoeman, F. D. (1992). *Privacy and social freedom.* Cambridge, England: Cambridge University Press.

Smith, M. R., & Marx, L. (1994). *Does technology drive history? The dilemma of technological determinism.* Cambridge, MA: MIT Press.

Tobias, M. W. (2014). Here's how easy it is for Google Chrome to eavesdrop on your PC microphone. *Forbes.* Retrieved from http://www.forbes.com/sites/marcwebertobias/2014/01/26/heres-how-easy-it-is-for-google-chrome-to-eavesdrop-on-your-pc-microphone/

United Nations. (2011). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* Retrieved from http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

United Nations. (2014). What are human rights? Retrieved from http://www.ohchr.org/en/issues/pages/whatarehumanrights.aspx

van Wel, L., & Royakkers, L. (2004). Ethical issues in web data mining. *Ethics and Information Technology*, *6*, 129–140. doi:10.1023/B:ETIN.0000047476.05912.3d

Woodward, C. (2003). Estonia, where being wired is a human right. *The Christian Science Monitor.* Retrieved from http://www.csmonitor.com/2003/0701/p07s01-woeu.html