

: How should digital ethics impact analytics and data mining?

by Ciara Heavin

and Daniel J. Power

Ethics should guide analytics, data mining, decision support, and decision making. Big data and new analytical tools have raised new ethical questions for managers. Ethics refers to "moral rules, codes, or principles which provide guidelines for right and truthful behavior in specific situations" (Lewis 1985, p. 382). Gartner (2018) defines digital ethics as "a system of values or moral principles for the conduct of digital interactions among people, businesses and things". Digital ethics creates a practical challenge for managers and most CIOs prioritize resolving digital ethics issues as a top priority in their digital strategies (Bhagyashree, 2018). Gartner identified digital ethics and privacy as one of its top strategic technology issues for 2019 (Lomass, 2018; High, 2018). Managers must address issues of compliance, risk mitigation, and values.

Values matter in decision making and digital transformation is creating new ethical dilemmas and value issues. As an issue is identified and resolved managers must develop policies related to the issue, develop compliance approaches, and reduce risks associated with non-compliance. While the broad issues of ethics, privacy and trust are not new for managers, people are increasingly concerned about their personal data and what happens to it once it is shared with a third party. Governments and companies need to address ethical issues related to technology and find methods to use data/information while designing best practices in order to respect people's privacy and maintain their trust.

The areas of big data analytics and data mining are relatively new, while information technology itself is ethically neutral, the decisions made by humans around information technology, data capture, and data analyses may give rise to ethical dilemmas. Big data analytics and data mining are among the information technology trends that have attracted attention from an ethics perspective. The Cambridge Analytica case is a recent very high profile example of unethical data mining of social media data to target and manipulate individual citizens with tailored election campaign ads. This scandal has required marketers, businesses and governments to rethink how new sources of data, i.e. social media data, are accessed, processed and used.

Gartner Fellow Frank Buytendijk (van der Meulen, 2017) identified four common ethical dilemmas in digital businesses: 1) privacy or profit, 2) future options versus appropriate use, 3) get it out versus get it right, and 4) needs of the many versus needs of the few. Buytendijk's labels or titles for these 4 dilemmas are very descriptive and self explanatory. Future options is somewhat vague but means collecting data that is not needed now, but may be useful or valuable in the future. In these situations, it may seem easy to choose privacy, appropriate use, get it right rather than get it out, and favor the needs of the many over the needs of the few. **But** in a dilemma situation, it may be much more complicated with trade-offs where an alternative choice involves losing a benefit or incurring a negative result in return for gaining another benefit.

: How should digital ethics impact analytics and data mining?

There is data protection and privacy legislation in place across jurisdictions, i.e. in the United States (data privacy laws like COPPA and HIPPA) and Europe (GDPR - General Data Protection Legislation). However, these laws vary greatly and there are gray areas in terms of how these laws are interpreted and enacted. New sources of data, new opportunities for data analysis, and data sharing requires citizens, business and governments to think and act beyond simple compliance when it comes to upholding a code of good digital ethics conduct. In order to achieve this goal, there is a real need for stakeholders to consider a number of ethical questions, including "just because we can do something, is it the right thing to do?", "what are the ethical implications?", "who will be affected?", and "what does doing this say about us as a person, business, or government agency?"

Clearly and Burke (2018) prescribe examining a hierarchy of intent to deal with and resolve digital ethics and privacy issues. The Clearly and Burke hierarchy includes four factors: 1) **Mind compliance** - this is the lowest level of the hierarchy, this factor is driven by legislation and the need to be in compliance, 2) **Mitigating risk** - some organizations may have a mindset of risk taking that may negatively impact the trust of customers if caught. It is important to consider negative consequences, e.g. losing customer trust, 3) **Making a difference** - making ethical decisions about data issues will have a positive impact on an organization's reputation, and 4) **Follow your values** - managers should make morally and ethically driven decisions about data capture, use, and retention. The moral acceptability of a decision and actions is an important criterion.

Compliance with laws and mitigation of risk factors are externally driven avoidance factors whereas making a difference and following one's values are considered internally driven achievement factors. The internal factors must become part of a culture of pursuing good digital ethical practices where organizations move from asking "are we being compliant?" to the more enlightened perspective of "are we doing the right thing?". To encourage and promote good practices and decision making related to digital ethical issues, we need to incorporate organizational strategies such as the Clearly and Burke hierarchy of intent and other best practice approaches to ensure we are first compliant and more importantly "doing the right thing" when it comes to leveraging big data analytics and data mining techniques when generating and sharing new data insights.

One way to incorporate privacy and an ethical mindset while designing algorithms and techniques for mining data is to leverage a "Privacy by Design" approach. Build privacy into processes and systems from the beginning. The concept of Privacy by Design is not new, cf., Dickie and Yule (2017). O'Connor et al. (2017) note "Privacy by Design promotes and demands that data controllers and processors are proactive in addressing the privacy implications of any new or upgraded system, procedure, policy or data-sharing initiative, throughout its planning phase and its full lifecycle (p. 644)".

Privacy by Design is based on the idea of Fair Information Practices (FIPs). The Code of Fair

: *How should digital ethics impact analytics and data mining?*

Information Practices (FIPs) was developed in the 1970s and based on five principles, cf., Dixon (2007). The principles in gender-neutral terms are:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information is in one's personal record and how it is used.
3. There must be a way for a person to prevent personal information obtained for one purpose from being used or made available for other purposes without that person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about her/himself.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Managers need to create and maintain the perception and reality of digital trust by clients, customers, employees, suppliers, government regulators, and other stakeholders. Digital trust is created and destroyed by every digital interaction. Managers should regularly measure and quantify stakeholder expectations to insure that reality and perception are accurate. An organization may be perceived like a "real" person and stakeholders need to be reassured about the claims and image and the anticipated and expected behavior of the organization. According to Swinhoe (2018), "Digital trust is the measure of consumer, partner and employee confidence in an organization's ability to protect and secure data and the privacy of individuals". The damage to an organization from losing digital trust can be enormous.

Digital ethics and Privacy by Design should be both guide and a focus for data scientists, data analysts, decision support analysts, managers, and IS/T professionals. Those charged with designing technological frameworks and solutions to counter the threats of undesirable, unethical attacks on privacy and trust violations must be diligent and vigilant. Digital ethics is about managing oneself and acting ethically and professionally using online and digital communications and digital storage mediums.

Ethical oversight and thoughtful policies must maintain an appropriate balance of interests. Data and analytics have the potential to impact people both positively and negatively. The dilemmas and trade-offs must be resolved for the overall benefits of society in general without harming individual rights. Data analysis of merged and combined data sets create both opportunities and serious

: *How should digital ethics impact analytics and data mining?*

ethical challenges. Managers should strive to build a culture that values ethical behavior. One hopes that in such a culture that win-win solutions like removing identifying particulars, and hence anonymizing data, can be found that will promote the knowledge discovery opportunities of big data analytics and data mining technologies. Building ethical considerations into analytics, data mining, and digital business is much better and easier than trying to add new policies, processes, and system updates later and as an after thought.

References

Bhagyashree, R. (2018). "Gartner lists Digital Ethics and Privacy as one of the top 10 strategic technology trends for 2019", Packt>, October 17 check URL
<https://hub.packtpub.com/gartner-lists-digital-ethics-and-privacy-as-one-of-the-top-10-strategic-technology-trends-for-2019/>

Cavoukian, A. and M. Chibba (2018). "Start with Privacy by Design in All Big Data Applications," Chapter 2 in S. Srinivasan (ed.), Guide to Big Data Applications, Studies in Big Data 26, pp. 29-48 DOI 10.1007/978-3-319-53817-4_2 at URL
<https://www.springer.com/cda/content/document/cda.9783319538167-c1.pdf>

Clearly, D. and B. Burke. (2018), "Gartner - Top 10 Strategic Technology Trends for 2019" at
<https://www.gartner.com/doc/3891569?refval=&pcp=mpe#>

Dickie N. and A. Yule. (2017). "Privacy by design prevents data headaches later," Strategic HR Review, 16(2), 100-101.

Dixon, P. (2007). "A Brief Introduction to Fair Information Practices," at URL
<https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>

High, P., "Gartner: Top 10 Strategic Technology Trends For 2019," Forbes, Oct 22, 2018 at URL
<https://www.forbes.com/sites/peterhigh/2018/10/22/gartner-top-10-strategic-technology-trends-for-2019/#2d7c06501423>

Lewis, P.V. (1985). "Defining 'Business Ethics': Like Nailing Jello to a Wall." Journal of Business

: *How should digital ethics impact analytics and data mining?*

Ethics, pp. 377–83. doi:10.1007/BF02388590.

Lomass, N. (2018). "Gartner picks digital ethics and privacy as a strategic trend for 2019", Feb 24, 2019 at URL
<https://techcrunch.com/2018/10/16/gartner-picks-digital-ethics-and-privacy-as-a-strategic-trend-for-2019/>

O'Connor, Y., Rowan, W., Lynch, L. and Heavin, C. (2017). "Privacy by Design: Informed Consent and Internet of Things for Smart Health," *Procedia Computer Science*, 113(Supplement C), pp. 653-658. doi: 10.1016/j.procs.2017.08.329 Published Version: 10.1016/j.procs.2017.08.329

Shetty, S. (2017). "Getting Digital Ethics Right: Interview with Frank Buytendijk," Gartner, June 6 at URL <https://www.gartner.com/smarterwithgartner/getting-digital-ethics-right/>

Swinhoe, D. (2018). "What is digital trust? How CSOs can help drive business," *CSO*, December 05, 2018 at URL
<https://www.csoonline.com/article/3297037/what-is-digital-trust-how-csos-can-help-drive-business.html>. CSO, Chief Security Officer, provides news, analysis and research on security and risk management.

University of Oxford (2018). The Oxford Uehiro Centre for Practical Ethics website at URL
<https://www.practicaethics.ox.ac.uk/ai-and-digital-ethics>

van der Meulen, R. (2017). "Kick-Start the Conversation on Digital Ethics: Four common digital ethical dilemmas are examined," *Smarter with Gartner*, October 13, 2017 at URL
<https://www.gartner.com/smarterwithgartner/kick-start-the-conversation-on-digital-ethics-2/>

An alternate statement: According to Gartner, "digital ethics is the system of values and principles a company may embrace when conducting digital interactions between businesses, people and things. Digital ethics sits at the nexus of what is legally required; what can be made possible by digital technology; and what is morally desirable...." at URL
<https://www.futuristgerd.com/2016/01/digital-ethics-the-role-of-the-cio-in-balancing-the-risks-and-rewards-of-digital-innovation/>

: How should digital ethics impact analytics and data mining?

Author: Daniel Power

Last update: 2019-03-23 02:49