What Is Morality? What Is Considered Morally Right Or Wrong Behavioral Business Ethics?

Posted on September 15, 2018

Introduction

Morality concerns the reasons people use to judge actions, character, institutions, and decisions as right, wrong, good, harmful, fair, or unjust. In business, moral questions appear whenever a decision affects employees, customers, investors, competitors, communities, or the public. Law and organizational policy provide important boundaries, but ethical responsibility cannot be reduced to legal compliance. A practice can be lawful and still deceptive or exploitative, while an unlawful act may sometimes be defended as civil disobedience against an unjust rule. Business ethics therefore requires disciplined judgment rather than a simple search for a rule that removes personal responsibility (Shaw, 2016; Schwartz, 2017).

The admissions-system incident discussed in the original essay provides a useful case. In 2005, instructions circulated online showing applicants to several business schools how to alter a web address and view admissions information before official release. Harvard Business School rejected 119 applicants who used the method. The episode raises questions about unauthorized access, curiosity, institutional security, proportional punishment, and the character expected of future business leaders. This essay explains morality, distinguishes it from law and etiquette, evaluates the incident through several ethical theories, and proposes a practical method for business decision-making (Harvard Crimson, 2005).

Morality, Ethics, and Business Conduct

Morality can refer to standards and practices through which people evaluate conduct. Ethics is often used for the systematic study of those standards. In ordinary conversation the words overlap, but the distinction is helpful: morality includes judgments and commitments, while ethical reasoning examines whether those judgments are coherent, justified, and fairly applied (Shaw, 2016).

Business ethics applies moral reasoning to commercial life. It asks not only whether a company can take an action but whether it should. Questions include whether advertising is truthful, wages are fair, data collection is proportionate, products are safe, taxes are responsibly handled, and environmental costs are transferred to people who receive little benefit. Individual conduct also matters. Employees and leaders decide whether to disclose conflicts, report misconduct, protect confidential information, honor commitments, or exploit a weakness in a system (Schwartz, 2017).

Ethics is not separate from competent management. Trust affects contracts, customer loyalty, employee retention, investment, and the ability to cooperate. A company that pursues short-term gain through deception may damage its long-term capacity to operate. Nevertheless, ethics should not be defended only because it is profitable. Some obligations remain even when violating them would produce financial advantage.

Morality and Law

Law establishes enforceable rules through legitimate institutions. It can express moral principles, deter harm, resolve disputes, and define minimum standards. Hacking, fraud, bribery, discrimination, and unsafe products may create legal as well as moral liability. Managers must understand applicable law because ignorance can harm stakeholders and does not ordinarily excuse violations (Shaw, 2016).

Yet legality and morality are not identical. Laws may be incomplete, outdated, weakly enforced, or unjust. A company can comply technically with a disclosure rule while designing the disclosure so that ordinary customers cannot understand it. An employer may use a contractual power in a way that is needlessly humiliating. Conversely, people have sometimes violated unjust laws to defend civil rights. Ethical judgment asks about reasons, consequences, rights, fairness, and character beyond the legal label (Shaw, 2016; Schwartz, 2017).

In the admissions case, whether every applicant's action satisfied the technical elements of a criminal offense is not the only issue. The users attempted to access information that the schools had not released to them. The absence of sophisticated code or a strong password did not create permission. Leaving a door poorly secured may reveal negligence, but it does not automatically authorize entry (Harvard Crimson, 2005).

Morality and Etiquette

Etiquette concerns social conventions such as greetings, dress, punctuality, and forms of politeness. Violating etiquette may be rude without causing serious moral harm. Moral rules usually protect deeper interests such as life, freedom, privacy, equality, honesty, and fair opportunity (Shaw, 2016).

The categories can overlap. Persistent humiliation disguised as a breach of manners may create a hostile workplace. Courtesy can express respect, and disrespect can support discrimination. Still, confusing etiquette with morality can cause organizations to punish harmless difference while overlooking fraud or exploitation. A quiet employee who dislikes formal networking is not ethically inferior to a charming executive who manipulates accounts.

Major Approaches to Ethical Judgment

Duty and Respect for Persons

A duty-based approach asks whether an action follows principles that could be applied consistently and whether it respects people as ends rather than tools. Honesty, promise keeping, confidentiality, and respect for autonomy are central duties. Accessing unreleased decisions uses the institution's system contrary to its intended authorization and gives the user an advantage unavailable to applicants who follow the process. The action is difficult to universalize: if every applicant accessed hidden material whenever a technical weakness allowed it, controlled notification would become impossible (Shaw, 2016; Schwartz, 2017).

Duty ethics also applies to the schools and their technology provider. They had obligations to secure sensitive records, test the system, communicate clearly, and respond fairly. The applicants' wrongdoing, if established, does not erase institutional responsibility for preventable design failures.

Consequences and Stakeholder Welfare

A consequentialist analysis evaluates likely benefits and harms. An applicant receives earlier knowledge and temporary relief from uncertainty. Against that benefit are privacy and security risks, unfair advantage, administrative disruption, loss of trust, and the possibility that normalized unauthorized access will encourage more harmful behavior (Shaw, 2016).

The consequences of punishment must also be considered. Automatic rejection may deter misconduct and protect institutional credibility, but it can be harsh when applicants differ in knowledge, intent, or who actually used the account. Stanford reportedly reviewed affected cases individually, illustrating an alternative approach. Consequential reasoning therefore supports preventing unauthorized access while still asking whether one sanction best fits every circumstance.

Virtue Ethics

Virtue ethics focuses on character. Business leaders need honesty, courage, fairness, humility, prudence, and accountability. The admissions incident tests what a person does when temptation is available and detection appears uncertain. Curiosity is understandable, but practical wisdom requires recognizing that available information is not necessarily authorized information (Schwartz, 2017).

Virtue analysis should avoid claiming that one mistake reveals a complete and permanent character. People can act poorly, learn, accept responsibility, and change. A fair institution examines conduct seriously without pretending to know an entire person from one event. The important questions include whether the applicant understood the action, concealed it, blamed others, or responded honestly when confronted.

Justice and Fairness

Justice asks whether benefits, burdens, procedures, and opportunities are distributed fairly. Applicants who accessed results early gained information that others did not have. Even if the decision itself was already made, equal treatment of applicants was disrupted. The schools also needed consistent procedures so that similarly situated people were treated similarly (Shaw, 2016).

Procedural justice includes notice, evidence, an opportunity to explain, impartial review, and proportionate consequences. An account may have been accessed by a family member without the applicant's knowledge; an individual may have followed ambiguous instructions without understanding what would be revealed. These possibilities do not excuse intentional access, but they justify reliable fact-finding rather than assumption.

Rights and Privacy

Applicants have rights to appropriate handling of their personal information, while institutions have rights to control access to internal systems. Other applicants have a legitimate interest in a fair process. Unauthorized access threatens all three. A rights-based view therefore condemns exploitation of the vulnerability and requires the schools to improve security and notification practices (Schwartz, 2017).

The 2005 MBA Admissions Incident

The method reportedly involved logging into an application account and changing part of the web address to reach a decision page before release. Because the flaw did not require advanced programming, some participants described their behavior as "peeking" rather than hacking. Ethical analysis should not depend entirely on the dramatic label. The key question is authorization. A person can obtain unauthorized access through a simple action (Harvard Crimson, 2005).

Harvard Business School rejected 119 applicants connected to the access. The school emphasized integrity and the responsibility of future leaders. Other schools took different approaches, including individual review. The variation reveals a genuine dilemma. Institutions need to communicate that exploiting systems is unacceptable, but sanctions should consider evidence, intent, consistency, and proportionality (Harvard Crimson, 2005; Harvard Business School, n.d.).

The incident also demonstrates shared responsibility. ApplyYourself and the schools failed to prevent predictable manipulation of the URL. Security design should assume that users may experiment. Sensitive decisions should remain inaccessible until release, and authorization should be enforced on the server rather than hidden behind an unadvertised address. Ethical organizations do not place all responsibility on users while ignoring their own insecure systems.

What I Would Do as an Applicant

If I encountered the instructions, the ethically preferable action would be not to use them. I would wait for the official decision and, if the instructions appeared credible, notify the school or platform without accessing another person's data or distributing the method. This response respects authorization, equal treatment, and the privacy of the system (Schwartz, 2017).

The decision would remain correct even if there were no risk of detection. Ethical integrity is tested precisely when external punishment is unlikely. It would also remain correct if the result could not be changed, because the ethical issue concerns the means of access and the norm being established, not only the content obtained.

If I had accessed the page impulsively, the responsible response would be to stop, preserve relevant facts, disclose the action honestly, and accept a fair review. Concealment would add deception to the original decision. Accountability does not guarantee forgiveness, but it demonstrates the capacity to learn.

A Practical Ethical Decision Process

Business decisions often occur under time pressure, uncertainty, and competing incentives. A structured process can reduce self-serving reasoning. First, define the decision accurately and identify what information is missing. Euphemisms such as "peeking," "creative accounting," or "growth hacking" can hide the moral character of an action (Schwartz, 2017).

Second, identify stakeholders, including people who are less visible or have less power. Third, determine legal, contractual, professional, and organizational obligations. Fourth, evaluate options through consequences, duties, rights, fairness, and character. A decision that appears acceptable under only one framework deserves further scrutiny.

Fifth, test consistency. Would the decision be defensible if every competitor used it, if it were reported publicly, or if the decision-maker were the affected party? Sixth, seek independent review when conflicts of interest or severe consequences exist. Finally, document the reasons, implement safeguards, and revisit the outcome. Ethical management is a learning process rather than a one-time declaration of values (Shaw, 2016; Schwartz, 2017).

Organizational Culture and Moral Responsibility

Companies influence conduct through incentives and examples. A code of ethics cannot overcome a compensation system that rewards results regardless of method. Leaders who quietly tolerate manipulation teach employees that stated values are ceremonial. Organizations need protected reporting channels, fair investigations, consistent sanctions, and recognition for responsible behavior (Schwartz, 2017).

Technology design is part of culture. Systems should apply least privilege, log sensitive access, protect confidential data, and make authorization boundaries clear. Employees should not be expected to compensate for insecure design through perfect behavior, but security controls cannot replace moral judgment. Effective governance uses both.

Moral disagreement is unavoidable in diverse organizations. The goal is not to pretend that every issue has an obvious answer. It is to create processes in which reasons can be tested, stakeholders heard, evidence corrected, and powerful actors held accountable.

Conclusion

Morality in business concerns justified standards of right action, fair institutions, and responsible character. It overlaps with law and etiquette but cannot be reduced to either. Ethical decisions require attention to duties, consequences, rights, justice, and virtues (Shaw, 2016; Schwartz, 2017).

The 2005 MBA admissions incident was morally significant because applicants used a system in a way that was not authorized to obtain unreleased information. The schools were justified in treating the conduct seriously, while they also had obligations to secure the system and apply fair procedures. The most ethical choice for an applicant was to wait, report the vulnerability responsibly, and refuse an advantage obtained through unauthorized access. For business leaders, the broader lesson is that integrity means choosing defensible methods even when a shortcut is easy, profitable, and unlikely to be discovered (Harvard Crimson, 2005; Harvard Business School, n.d.).

Works Cited

Shaw, William H. (2016). *Moral Issues in Business*. 13th ed., Cengage Learning.

Schwartz, Mark S. (2017). *Business Ethics: An Ethical Decision-Making Approach*.

Harvard Crimson. (2005). HBS to reject snooping hopefuls.

Harvard Business School. Admissions integrity and procedures.