Is Whistleblowing Ethically Justified in IT When Internal Reporting Fails and User Harm Is Likely?

Whistleblowing is one of the hardest ethical issues an IT professional faces. It often conflicts with company policy or confidentiality agreements. IT professionals are expected to be loyal to their organizations. At the same time, they have responsibilities to users and the public. The main ethical issue is deciding when preventing harm matters more than loyalty to an employer.

Whistleblowing is ethically justified when an organization's actions cause serious harm or pose a clear risk of harm. This includes illegal data collection, privacy violations, or ignored security risks. When these actions continue, users face real harm. In these cases, remaining silent becomes ethically wrong (Tavani, 2021).

Another key factor is the use of internal reporting channels. Ethical guidance states that concerns must first be reported internally. This includes supervisors, compliance teams, or ethics hotlines. When these efforts are ignored or covered up, whistleblowing becomes ethically defensible. In these situations, confidentiality agreements protect wrongdoing instead of the public interest (Near & Miceli, 1985).

Ethical theories help explain this issue. From a utilitarian view, whistleblowing is ethical if it prevents greater harm and benefits more people. A deontological view focuses on honesty and respect for individual rights. This duty applies even when company rules discourage disclosure. Moor's just-consequentialism supports whistleblowing when the outcome is fair and prevents unjust harm (Moor, 1999).

Professional standards also support these responsibilities. The ACM Code of Ethics states that computing professionals must avoid harm and act in the public interest, even under pressure from an employer (ACM, 2018). This shows that loyalty to a company does not outweigh responsibility to society.

Whistleblowing remains a last option. It requires strong evidence, ethical intent, and a clear risk of harm if no action is taken. When these conditions exist, whistleblowing is ethically justified despite violating company policy.

References

Tavani, H. (2021). *Ethics and Technology* (5th ed.). Wiley.

Moor, J. H. (1999). *Just Consequentialism and Computing*. Ethics and Information Technology.

ACM. (2018). *ACM Code of Ethics and Professional Conduct*.

Near, J. P., & Miceli, M. P. (1985). *Organizational Dissidence: The Case of Whistle-Blowing*. Journal of Business Ethics.

My Response

Iqra, you've identified the core tension perfectly, the conflict between organizational loyalty and public responsibility when internal reporting fails. Your framework aligns well with what our lecture materials describe as "divided loyalties," where IT professionals must balance competing obligations to employers, professional codes, and society. I want to build on your argument by introducing some complications that emerged in our Week 3 readings, particularly around **who** bears the whistleblowing obligation when responsibility is organizationally diffused, and **what threshold** of harm triggers that obligation in technology contexts.

The "Many Hands" Problem and Individual Obligation

You argue that whistleblowing becomes justified when "these efforts are ignored or covered up," but Nissenbaum's (1994) concept of the "problem of many hands" complicates this in interesting ways. In large technology companies, harmful outcomes emerge from complex systems involving thousands of engineers, product managers, executives, and algorithms, each contributing small pieces to a larger harmful system. Nissenbaum explains that traditional responsibility models struggle here because harmful outcomes can't be traced to any single individual's decisions or actions. When a recommendation algorithm amplifies misinformation, for example, the training data came from one team, the model architecture from another, the engagement metrics from product management, and the business decision to prioritize engagement over accuracy from executives. **If you're a mid-level engineer who can see how these pieces fit together to create harm, does your specialized knowledge create a *heightened* individual obligation to whistleblow, or does organizational complexity actually *distribute* responsibility in ways that reduce what any single professional should be expected to risk?** This isn't just theoretical; it directly affects whether we can reasonably expect individuals to bear the personal and professional costs of whistleblowing (job loss, blacklisting, legal retaliation) when dozens or hundreds of people contributed to the harmful outcome.

What Counts as "Serious Harm" in Technology Contexts?

Your utilitarian and deontological analysis is compelling, but I think we need to wrestle more explicitly with the **harm threshold question** that our lecture materials raised. You mention "illegal data collection, privacy violations, or ignored security risks" as clear harms, which aligns with De George's (1999) first criterion that "the harm that will be done by the product to the public is serious and considerable." But De George was writing primarily about traditional engineering contexts where harm meant physical injury or death—bridges collapsing, medical devices malfunctioning, aircraft systems failing. **When Frances Haugen disclosed Facebook's internal research showing Instagram's documented negative effects on teenage girls' mental health, the harm was real but psychological and social rather than physical** (Horwitz & Seetharaman, 2021; U.S. Senate, 2021). The internal documents showed 13.5% of teen girls in the UK and 6% in the US said Instagram made suicidal thoughts worse, and that Instagram made body image issues worse for one in three teen girls. Is this level of psychological harm at massive scale (tens of millions of users) equivalent to the "serious and considerable" physical harm De George contemplated? **How do we operationalize "seriousness" when the harm is informational, psychological, or democratic rather than physical, and does the *scale* of impact (billions of users) change the moral calculus?**

Exhausting Internal Channels in Practice

You correctly note that "concerns must first be reported internally" before whistleblowing becomes defensible, which tracks De George's criteria about exhausting channels "including going to the board of directors." But I'm curious about what this means **in practice** at large technology companies with complex hierarchies, legal departments incentivized to minimize liability, and executives with financial stakes in maintaining harmful but profitable systems. The lecture materials note that Haugen testified she felt she had exhausted internal channels before going to the SEC and Congress, but Facebook's leadership disputed this characterization. **At what point do we consider internal channels truly "exhausted", when you've reported to your immediate manager who dismissed concerns? When you've escalated to senior leadership who acknowledged the problem but deprioritized fixes? When you've gone to the board of directors who deferred to management's business judgment? Or only when you've filed formal complaints through every possible internal mechanism and waited months or years for responses that may never meaningfully come?** This isn't just procedural; the Sarbanes-Oxley Act (2002) and Dodd-Frank Act (2010) provide some legal protections for whistleblowers, but those protections have significant gaps and enforcement has been inconsistent (Kohn, 2011). If "exhausting internal channels" in practice means spending 18-24 months in internal bureaucratic processes while harmful systems continue affecting millions of users daily, does that timeline itself become ethically problematic?

My question for you and others: How would you operationalize these criteria into a practical decision framework that IT professionals could actually use when facing these dilemmas? What specific evidence thresholds, timeline expectations, and organizational conditions would need to exist before whistleblowing shifts from "permissible" to "obligatory" in your view, and how should that framework account for the reality that whistleblowers face severe personal and professional consequences even when they're ultimately vindicated?

Refernces

De George, R. T. (1999). *Business ethics* (5th ed.). Prentice Hall.

Horwitz, J., & Seetharaman, D. (2021, September 14). Facebook knows Instagram is toxic for teen girls. *The Wall Street Journal*. https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

Kohn, S. M. (2011). *The whistleblower's handbook: A step-by-step guide to doing what's right and protecting yourself*. Lyons Press.

Nissenbaum, H. (1994). Computing and accountability. *Communications of the ACM*, *37*(1), 72–80. https://doi.org/10.1145/175222.175228

U.S. Congress. (2002). *Sarbanes-Oxley Act of 2002*. Pub. L. No. 107-204, 116 Stat. 745.

U.S. Congress. (2010). *Dodd-Frank Wall Street Reform and Consumer Protection Act*. Pub. L. No. 111-203, 124 Stat. 1376.