TECH ETHICS:
Best Practices

MARKKULA CENTER FOR APPLIED ETHICS
at Santa Clara University

Tech Ethics: Best Practices

Shannon Vallor, Regis and Dianne McKenna Professor, Santa Clara University
with Brian Green, Director of Tech Ethics, Markkula Center for Applied Ethics

What are ethical 'best practices' in technology?

'Best practices' is a term often used in contexts where it is very important that the thing be done well, and where there are significant costs or risks to doing it in a less than optimal way.

Here we describe best practices for the process of incorporating appropriate ethical attention, reflection, and decision-making in the context of technology development.

No single code of technology ethics can fit all contexts and practitioners; organizations and professions should therefore develop explicit internal policies, procedures, guidelines, and best practices that are specifically adapted to their own activities and challenges. However, those specific codes of practice can be shaped by reflecting on these 16 broad norms and guidelines for ethical practice.

1. Keep Ethics in the Spotlight—and Out of the Compliance Box: Ethics is a pervasive aspect of technological practice. Because of the immense social power of technology, ethical issues are virtually always in play. Even when our work is not directly client-facing, ethical issues are never absent from the context. However, the 'compliance mindset' found in many organizations can, when applied to technology, encourage a dangerous tendency to 'sideline' ethics as an external constraint rather than see it as an integral part of being good at what we do. Law and ethics are not the same. What is legal can be unethical (quite common), and what is ethical can (even if less commonly) be illegal. If we fall victim to the 'compliance' mindset when we are thinking about ethics, we are more likely to view our ethical obligations as a box to check off and then forget about, once we feel we have done the minimum needed to 'comply' with them. Unfortunately, this often leads to disastrous consequences. Because ethical considerations are ubiquitous and intrinsic to tech development, our individual and organizational efforts must strive to keep the ethics in the spotlight.

2. Highlight the Human Lives and Interests behind the Technology: Especially in technical contexts, it's easy to lose sight of what technology actually does to human lives and interests. Even when the technology involves non-human entities (for example, recordings of ocean temperatures), it's being employed for important human purposes and interests. And much of technology involves the most sensitive aspects of human beings' lives: their bodies, their finances, their social relationships, and their emotional and mental states. A decent human will handle another person's body, money, or mental condition with due care; the same ethical duties apply when developing technologies that touch these and other important aspects of people's lives.

3. Consider Downstream (and Upstream and Lateral) Risks for Technologies: We often focus too narrowly on whether we have complied with ethical guidelines, and we forget that ethical issues concerning technology don't just go away once we have diligently performed our own particular tasks. It is essential to think about what happens to devices, software, hardware, or data after it leaves our hands. Even if, for example, we have done extensive testing of a product before its release, there are always new threats that can emerge, and new applications of the product that might create new challenges. We should always therefore have a view of the risks downstream from our practice, and maintain effective lines of communication with those in a position to monitor what happens to the product. Communication with those 'upstream' and lateral to our practice is also essential; if the reason that we struggle with keeping a technology functioning and interacting with society in an ethical manner is that poor design and configuration choices upstream are tying our hands, or because someone in another department is continually ignoring or overriding the practices we've instituted, then we need to be prepared to address that. If we are not paying attention to the downstream, upstream, and lateral risks, then we have not fully appreciated the ethical stakes of our own current practice.

4. Don't Discount Non-Technical Actors, Interests, and Expectations: Technologists are highly skilled in specific areas of technical practice and accustomed to interacting with others with similar levels of technical expertise. This can lead to a dangerously insular mindset when it comes to considering the interests of non-technical actors and risks to which they are exposed. It can also foster an ethically callous attitude toward people whose exposure to risks results from technical incompetence or naïvete. This attitude leads to missed opportunities to implement basic risk prevention and mitigation strategies, increasing the overall risk to the organization and third parties. Moreover, being technically naïve is not, in fact, something that makes a person any more deserving of harm or injury, or any less deserving of security. Maintaining appropriate empathy for non-technical actors and their interests will ultimately make you a better technologist.

5. Envision the Technical Ecosystem: We need to keep in mind the full context in which the technology we are working on exists now, and for what purpose, as well as keep in mind where the technology we handle today will be going tomorrow. For example, technologists handling a large dataset of medical records might be inclined to focus narrowly on how they will collect and use the data responsibly. But they also have to think about who else might have an interest in obtaining such data, and for what other purposes. They may also have to think about the cultural context in which they are collecting the data, which might embody expectations, values, and priorities that conflict with those of the technologists. In fact, technology practices are never isolated from a broader socio-technological ecosystem that includes powerful social forces and instabilities not under our control; we must consider our ethical practices and obligations in light of that bigger picture.

6. Mind the Gap between User Expectations and Reality: When developing technology, keep in mind how the stakeholders' expectations of a particular product may diverge from reality. For example, do users know enough about the risks of this technology? Might certain disclosure and use notifications lead to inflated expectations about how safe users are? Can we keep all the promises we have made to our users? For example, might we one day sell our product and/or its

associated data to a third-party who may not honor those promises? Often we make the mistake of regarding parties we contract with as equals, when we may in fact operate from a position of epistemic advantage—we know a lot more than they do. Agreements with subjects who are 'in the dark' or subject to illusions about the nature of the data agreement are not, in general, ethically legitimate.

7. Avoid Hype and Myths around Technology: We also need to remember that technology is powerful, but it isn't a silver bullet for complex social problems. There are, however, significant industry and media incentives to portray technology as exactly that. This can lead to many harms, from unreasonable product development goals to unrealized user expectations that can easily lead to backlash. Not all problems have technological solutions, and we may overlook more economical, ethical, and practical solutions if we believe otherwise. We should remember the joke about the drunk man who, when asked why he's looking for his lost car keys under the streetlamp, answers 'because that's where the light is.' For some problems, the best solutions may lie outside the 'light' of our technological focus.

8. Establish Chains of Ethical Responsibility and Accountability: In organizational settings, the 'problem of many hands' is a constant challenge to responsible practice and accountability. To avoid a diffusion of responsibility in which no one on a team may feel empowered or obligated to take the steps necessary to ensure effective and ethical practice, clear chains of responsibility must be established and made explicit to everyone involved in the work--at the earliest possible stages of a project. We should clarify who is responsible for each aspect of ethical risk management and prevention of harm, in each of the relevant areas of risk-laden activity. We should also make clear who is ultimately accountable for ensuring an ethically executed project or practice. Who will be expected to provide answers, explanations, and remedies if there is a failure of ethics or significant harm caused by the team's work? Established chains of responsibility and accountability ensure that members of a project or organization take explicit ownership of the work's ethical significance.

9. Treat Technology as a Conditional Good: Some of the most dangerous practices in tech involve treating technological development as an unconditional good. Technological progress is not, in itself, naturally going to lead to a better world. Rather, it is *how a technology is used* that will determine whether that technological development will lead to a better world. Nuclear weapons, for example, were an incredibly powerful technological advance, but since their development have cast a long shadow across civilization. For a more contemporary example, devices that can store more data can exacerbate privacy and security risks by enabling a careless mentality of "collect and store it *all* now, we'll figure out what we actually need later." Technology is a *conditional* good— it is only as beneficial and useful as we take the care to make it.

10. Practice Disaster Planning and Crisis Response: Most people want to focus on the positive potential of a project or system. While this is understandable, the dangers of this attitude are well known, and have often caused failure, disaster, or crisis that could easily have been avoided. This attitude also often prevents effective crisis response, when no one has planned for a worst-case-scenario. Civil and mechanical engineers, whose designs greatly impact public safety,

have long had a culture of encouraging forethought about failure. Understanding how a product or system will function in non-ideal conditions, at the boundaries of intended use, or even outside those boundaries, is essential to building in appropriate margins of safety and developing a plan for unwelcome scenarios. Thinking about failure makes technologists' work better, not worse. Crisis plans should be intelligent, responsive to public input, and most of all, able to effectively mitigate or remedy harm being done.

11. Promote the Values of Autonomy, Transparency, and Trustworthiness: To create and maintain a healthy relationship between technologists and the public, respect for autonomy, transparency, and trustworthiness is key. There are, unfortunately, numerous examples of lack of such respect: hiding risk behind legal, technical or PR jargon, disempowering users' efforts to promote their own wellbeing; vacuuming up data without appropriate consent and protections for what is collected; or burying a vulnerability or breach notification in order to try to spare oneself professional or public consequences, to name just a few. Of course, we can't always be completely transparent about everything we do. Likewise, sometimes the autonomy of users will be in tension with our obligations to prevent harmful misuses of technology. Occasionally, rhetoric about 'tensions' and 'balancing goods' may itself amount to unjust 'rationalization' or 'motivated reasoning' (believing something only because it benefits me to do so, or because I strongly wish it were true.) Nevertheless, balancing important rights and ethical values is not the same as sacrificing these values or ignoring their critical role in sustaining public trust.

12. Consider Disparate Interests, Resources, and Impacts: Technological practices carry a profound risk of producing or magnifying disparate impacts; that is, of making some people better off and others worse off (whether in terms of their social share of economic well-being, political power, health, justice, or other important goods.) Not all disparate impacts are unjustifiable or wrong. For example, while a device that uses strong end-to-end encryption may make it easier for criminals to avoid government scrutiny of their communications, it may also have a disparate impact on authoritarian governments' ability to track and neutralize their political opposition. Here, the ethical balance of the disparate impacts is quite complex (as seen in 2016's case of Apple v. the FBI.) But imagine another device that offers cutting-edge security tools and features only to those buying the most expensive model, and outdated/weak security features in all other models. Can the disparate impact of this choice be justified? The ethical risk from disparate impacts must be presumed; those impacts must be anticipated, actively audited for, and carefully examined for their ethical acceptability.

13. Design for Privacy and Security: This might seem like an obvious one, but its importance can't be overemphasized. 'Design' here means not only technical design (of networks, databases, devices, platforms, websites, tools, or apps), but also social and organizational design of groups, policies, procedures, incentives, resource allocations, and techniques that promote privacy and security objectives. The implementation will vary depending on context, but the essential thing is that the values of privacy and security should remain at the forefront of project design, planning, execution, and oversight--never treated as marginal, external, or 'after-the-fact' concerns.

14. Invite Diverse Stakeholder Input: One way to avoid 'groupthink' in ethical risk assessment and design is to invite input from diverse stakeholders outside of the team and organization. It is important that stakeholder input not simply reflect the same perspectives one already has within the organization or group. Often technologists have unusually high levels of educational achievement and economic status, and, in many technical fields, the representation of the population in terms of gender, race, ethnicity, age, disability, and other characteristics is skewed. Also, the nature of the work may attract people who have common interests and values--for example, a shared optimism about the potential of science and technology, and comparatively less faith in other social mechanisms. All of these factors can lead to organizational monocultures, which magnify the dangers of groupthink, blind spots, and poor design. For example, many of the best practices above couldn't be carried out successfully if members of a team struggled to imagine how a technology would be perceived by, or how it might affect, people unlike themselves. Actively recognizing the limitations of a team perspective is essential. Fostering more diverse tech organizations and teams is one obvious way to mitigate those limitations; soliciting external input from a more truly representative body of those likely to be impacted by our practice is also extremely important.

15. Make Ethical Reflection & Practice Standard, Pervasive, Iterative, and Rewarding: Ethical reflection and practice is an essential and central part of professional excellence in technology, yet it is still not fully or consistently integrated into technological practice. The work of making ethical reflection and practice standard and pervasive must be carried out through active measures taken by individual practitioners and organizations alike. To be effective, ethical reflection and practice must also be instituted in iterative ways. Because technologies are continually evolving, we must treat technology ethics as an active and ongoing learning cycle in which we continually observe the ethical outcomes of our practices, learn from our mistakes, gather more information, acquire further ethical and technical expertise, and then update and improve our practice accordingly. Most of all, ethical practice in technology must be made *rewarding*: aligning team and institutional/company incentives with ethical best practices will reinforce those practices and empower practitioners to carry them out.

16. Model and Advocate for Ethical Tech Practice: One way to be guided well in practical ethical contexts is to find and pay attention to excellent models of that practice. Eventually, becoming excellent oneself not only allows you to guide others--it also allows you to collaborate with other excellent persons and professionals, to improve the standards by which we all live. Aspiring technologists can benefit from seeking, identifying, and developing strong mentoring relationships with excellent models of ethical tech practice—models who not only possess technical excellence, but who are also exemplars of ethical leadership. A diverse range of models to learn from is best, as even experts have their weaknesses and blind spots. But those who develop practical wisdom by learning from the best mentors can in turn become excellent mentors to others, raising the overall excellence and nobility of the field. Jointly, they can also work to advocate for more technically and ethically superior norms, standards, and practices in the field, raising the bar for everyone, and ensuring that technologists help to secure and sustain the promise of a flourishing world for us all.

This document is adapted from the following sources:

Vallor, Shannon. "An Introduction to Cybersecurity Ethics." *Markkula Center for Applied Ethics Website*, February 7, 2018, pp. 48-52. Available at: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf

Vallor, Shannon. "An Introduction to Data Ethics." *Markkula Center for Applied Ethics Website*, January 23, 2018, pp. 48-52. Available at: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToDataEthics.pdf