The practice of ethics has not traditionally been a part of software development. Software didn't always have a direct impact on daily life, and the pace of development was slow. In modern society, people encounter software in all aspects of life, and big data and data analytics have real ramifications for individuals.

Although software developers work primarily behind the scenes in businesses, their decisions in the course of a project can have an outsized impact in the world -- for better or worse. Everyone in the industry should be aware of social and ethical issues in software development. Here are five examples of ethical issues and how developers can address them:

* addictive design;
* corporate ownership of personal data;
* algorithmic bias;
* weak cyber security and personally identifiable information (PII) protection; and
* overemphasis on features.

Addictive design

Every developer yearns to create applications that people love to use -- that's just good UX design. The problem is that some teams craft apps that people love too much. There is an ethical concern about the role of digital platforms, such as social media.

"As long as social media companies profit from outrage, confusion, addiction and depression, our well-being and democracy are at risk," argue critics like Tristan Harris of the Center for Humane Technology. Harris notably went viral while at working Google, with a presentation about the push for addictive technology design and companies' moral responsibility in society.

Striking an ethical balance between products consumers love and products that hijack their attention is more an art than a science. In product creation and updates, ask the following questions:

Who benefits?

How do they benefit?

To what degree do they benefit?

Are there safeguards for user health and sanity?

How overt is monetization and customer data collection and use, including via AI and machine learning (ML)? How transparent are these practices?

Explore addictive design, suggests David K. Bain, vice president of standards for the Telecommunications Industry Association, by comparing popular apps like Duolingo and TikTok. Both apps generate growth and revenue for their creators, but the nature of their benefit to users is different. Duolingo's clients gain language skills and are challenged with activities that enhance neuronal growth and brain plasticity. TikTok users receive cultural knowledge as well as immediate gratification with video content that bathes the brain with intoxicating neurotransmitters. "Based on this, many adults would say that the true user benefit of Duolingo is greater than [that of] TikTok," Bain said, but added that his 15-year-old daughter would disagree.

The two apps have different attitudes toward usage limits meant to safeguard against addictive attachment. Duolingo encourages consistency and makes the strong case that its use is linked to optimized learning curves. Duolingo definitely grabs users by the lapels to meet their daily quota and maintain performance streaks. But once the daily activities are done, Duolingo releases the user. By contrast, TikTok entices users to stay with an essentially limitless buffet of consumable media.

Apps often include user manipulation, monetization methods, user data collection for corporate use and machine learning algorithms to enhance the app. Transparency means what the users actually know and understand about these practices. Here's how this ethical aspect plays out in the two example apps:

"Duolingo's users are clearly willing victims of an enforced daily regimen, but are most certainly not aware that ads and usage data connect to a much larger advertising ecosystem," Bain said. "TikTok's users, especially the younger ones, I am quite sure are largely and happily oblivious to the methods and outcomes of their addictions."

Questionable personal data ownership

AI-based processing of biometric and other contextual data about customers has increased exponentially with device and software evolution. Software can profile users and predict behaviors at a scary level of detail.

"Usually, the ethical question is [one of] what to do with that data," said Miguel Lopes, vice president of product line management at Vidyo, a video conference platform. This ethical issue is a dilemma for developers in every kind of business -- not just the social media giants who make the news.

An algorithm directs information collection and building a profile, but the subsequent actions are intentional, and the developer is ordinarily aware of the power of this data in context.

One of the root causes of ethical concerns relates to how the business generates revenue and incentivizes developers and business managers, Lopes argued. In many cases, companies look at user data as a valuable currency, and want to monetize the data they store. "These factors might cause these organizations to share their user data unethically," Lopes said.

Developers face a hard decision regarding personal data and software design. They can create systems to exploit user data with the understanding that the liability lies with the organization, or they can raise concerns but face potential penalization for going against the project's aims. Modern technology companies' working culture should let developers come forward with personal data ownership concerns without fear of retaliation.

These kinds of concerns galvanized some rich discussion at Vidyo, which decided not to offer a free service tier. "We have analyzed the implications and prefer to sustain our operations by selling our service instead of our user data, and not subjecting our developer team with these difficult choices," Lopez said. The company has also found that transparency, internally, is a crucial factor. Developers should be aware of the entire context of the project they are working on, not just the module they need to complete.

Companies should make it easy for developers to step forward with concerns. The HR department could create mechanisms where developers can express their concerns without the fear of retaliation, such as an anonymous hotline for ethical concerns. The organization should then follow up and independently identify if the use case is in breach of privacy, legal or ethical policies.

Algorithmic bias

Technology can amplify existing biases. "One of the more pressing ethical issues facing today's developers is bias," said Spencer Lentz, principal, AI and digital process automation, digital customer experience, at consulting firm Capgemini.

Bias often enters the system undetected -- Lentz compares bias to a virus. Computers themselves have no inherent moral framework. Software can only learn from the training it is given. Therefore, developers and data scientists must scrub bias from the training data and the algorithms they build. From a developer's perspective, bias often centers on eliminating options for the wrong reasons, Lentz said.

Reporting and research in recent years illustrates how bias within software systems can perpetuate systemic racism against specific populations, which creates lost opportunity, worsens medical care and increases rates of incarceration. For example, in the book, Race After Technology, Ruha Benjamin raised some concerns about a case where developers failed to include Black people's voices in training AI speech recognition algorithms, under the belief that fewer Black people would use the app.

Anaconda, a data science platform, conducts the "State of Data Science Survey" and in 2020 found that 27% of data practitioners thought the biggest problem to tackle in AI and ML was the social impact from bias in data and models.

"To reduce bias in data and models, practitioners must be intentional about their work, asking questions like 'How was this data collected,' and 'What assumptions were collected with it,' said Peter Wang, CEO and co-founder of Anaconda. "If you don't know how the data that trained your models was collected and under what conditions, then your models could inadvertently perpetuate biases in their outputs." Executives, data scientists and developers must create an organizational culture that establishes ethical guidelines and empowers individuals at any level of the business to speak up if they see something problematic.

It's time to create a governing body, similar to the American Medical Association for doctors, Wang argued. This body could establish industry-wide ethical guidelines and best practices. "These technologies are still relatively new in the business context, and we would all benefit from ethical standards derived from our collective intelligence and input, rather than leaving it up to each individual or organization to decide for themselves," he said.

Weak security and PII protection

Application security is growing in importance as software plays a larger role in our online and offline environments.

Developers often only address security after code release, rather than during development. As a result, the software community lacks secure development standards. "The emphasis is almost entirely on getting a product out to market," said Randolph Morris, CEO of Bit Developers, a software development consultancy. Once a software product is publicly available, the focus shifts to new features and performance optimization, so security continues to have minimal prominence.

Hackers and other malicious actors cause real damage to real people. Our current digital ecosystem tends to address application security by plugging vulnerabilities as they are found. The reactionary approach is neither practical nor pragmatic.

To address this ethical responsibility for customer safety, developers need education, but typically only cybersecurity-specific classes address these topics. To start, educate your team about cybersecurity failures such as the Anthem medical data breach in 2015, where PII was stored as plain text in a database. "If this information was encrypted, it would not have been so easy to use and valuable to distribute," Morris said.

Also, the industry needs revised security standards. Organizations can do more to embrace standards meant to protect PII. The Payment Card Industry Data Security Standard and HIPAA for health apps are a good start, but developers should consider other forms of PII as well, and software designs that protect it.

Prioritizing features over impact

At the center of many ethical issues is a decision that capabilities in software releases are more important than the effects they could have. But just because you can doesn't mean you should.

"If the development team is measured on their rate of feature development, there's a high probability that the ethics of a given implementation might not be front of mind, either at the design or at the implementation phase," said Tim Mackey, principal security strategist at Synopsys Cyber Security Research Center. Synopsys is an electronic design automation company.

The business itself must set the tone for ethical standards in its software. Reflect ethics priorities throughout software lifecycle from design to operation. Train staff on ethical choices such as open source software licensing and use. Teach developers, architects, testers and other software team members about data management practices that comply with regulations and customer expectations. Developers don't follow news on the latest legislative actions in the jurisdictions where customers use their software, Mackey pointed out, but the business must ensure they're informed.

Collaboration between engineering leadership and legal teams can avoid ethical shortcomings. For example, the business should focus on customers' personal data access and retention. Data access controls and logging mechanisms are enabled at software implementation time. Developers -- tasked with creating a functional, user-friendly product -- will view data access restrictions as the responsibility of another team. Instead, ensure data protection is a feature included in the software design, inherently protecting against unauthorized access.