

Real life dilemmas

1. AI is a major money making technology, on the crest of a wave for tech futures for a few years now and not going away anytime soon. It is the future for us all. Major investment is taking place, by the billions of dollars at a time.

Statista estimates a massive USDollars 126 billion in revenue from AI-enabled apps by this year (2025).

In 2020, Timnit Gebru, a researcher in AI and ethics at Google, was allegedly sacked for highlighting a lack of diversity in the AI research at Google and a bias in AI facial recognition. Gebru had evidence of a high error rate of AI when analysing faces of women of colour. Gebru felt an ethical priority to ensure technology used to identify people was fit-for-purpose for all, not just white faces. Her decision put the investment and stock prices of Google at risk.

This is an example of an ethical dilemma faced by IT professionals.

If you were in Gebru's position, would have done the same?

Even if it meant you losing a high paid dream job?

What are the repercussions?

What else could have been done?

2. Security professionals are often on the firing line of security risk, even losing their jobs because of breaches. For example, San Francisco State University suffered a major data breach in 2014, exposing many student records. An information security officer at the university, Mignon Hoffman, was sacked after the breach. Hoffman alleged that the university sacked her for disclosing the security failings of the university — in other words, she chose to become a whistleblower as the most ethical thing to do. As a result, Hoffman sued the university for "wrongful termination and whistleblower retaliation."

Hoffman felt that telling the truth was an important ethical decision. However, she paid the price by losing her job. Whistleblowing is protected by law in the U.S. The decision to blow the whistle on bad practices can be complex and contextual, but some security issues are just too big to ignore. Such was the case when Edward Snowden blew the whistle on the surveillance activities of the NSA back in 2013. Snowden paid a heavy price, having to leave his home country. He said in the first documents he provided, "I understand that I will be made to suffer for my actions," but "I will be satisfied if the federation of secret law, unequal pardon and irresistible executive powers that rule the world that I love are revealed even for an instant."

Sometimes an ethical decision is a no-brainer. But would you have given up your home to highlight state wrongdoings?

3. A question of ethics.

Technology is not just about having the latest gadget: Tech is deeply integrated into our lives. Social media and other online interactions can have a real-life impact on our society's governance. Technology has the potential to create a more inclusive society or, conversely, to divide and conquer. Technologies can magnify inequalities when poorly designed or the harm they could inflict is not considered. Cybersecurity, privacy and digital identity are at the intersection of ethical software design, development and use.

When security professionals engage in pentesting or hardening security systems or have privileged access to perform their roles, they may encounter the types of ethical dilemmas mentioned above. But understanding the complex nuances behind ethical decisions is not a black-or-white issue. One person's ethical choice is another's missed opportunity. Because of this, ethical issues must be part of general education in cybersecurity for all security professionals. We are all human, and being ethical is always challenging. Hopefully, our decisions are the right ones.

Perhaps cybersecurity professionals should take an oath, as our medical counterparts have, that says we will "do no harm."

What do you think?