Task 3A

Asset protection in organizations is done through a combination of legal and technological aproaches with respect to both tangible and intangible resources . Prominent among these is the use of intellectual property, including copywrites, patents, and trademarks. Copywrites protect original works such as music, literature, or software; therefore, owners have exclusive rights to the materials. Patents alow the inventor to have exclusive rights to their new invention, enabling them to benefit from it without having competitors copying. Many pharmaceutical companies protect their drug formulas through patents. Trademarks, such as the Nike swoosh or Apple's logo, identify a firm's brand and help customers differentiate their products from others.

Besides that , NDAs are applied when companies need to disclose confidential information to employees or partners. The agreements legally prevent the receivers from sharing or reusing the sensitive information .

Technologically, watermarks are methods that companies use to embed hidden or visible information in images or documents to prove ownership. Software licenses, on the other hand, refer to control policies on how a user can access and use software; Digital Rights Management (DRM), often simply called DRM , refers to ways of controlling unauthorized copying or distribution of digital content, such as e-books and music . Lastly, software protection dongles are physical devices that allow access to software but prevent unauthorized users from using it .

Together, these legal and technological measures help secure the intellectual and creative property of companies from unauthorized use and exploitation .

Task 3B

Information wants to be free

"Information wants to be free" has been the battle cry of those advocating for free access to knowledge and data. Unfortunately, this idealism clashes with the proprietary interests of organizations that see information as a commodity to be controlled and monetized. Two recent cases—one involving DRM and another involving NDAs—illustrate the tension between these competing interests.

DeCSS is a software program developed in 1999 that bypasses a type of DRM called CSS , which prevents the copying of DVDs. The creator, Jon Lech Johansen , explained that DeCSS was needed so that individuals could play DVDs on open-source operating systems like Linux . Despite the entertainment industry's efforts to suppress DeCSS, Johansen was acquitted, highlighting the ongoing conflict between proprietary control and consumer rights.

Another example is the Waymo vs. Uber case, which demonstrates the tension between proprietary control and public access. Waymo, the self-driving car division of Alphabet , accused Uber of stealing trade secrets related to its technology. The central figure, Anthony Levandowski , a former Waymo engineer, had signed an NDA with the company. It was alleged that Levandowski downloaded approximately 14,000 confidential files before leaving

Waymo to found a self-driving truck startup that was later acquired by Uber.
It also accused Uber of misappropriating the stolen trade secrets in violation of Levandowski's NDA with Waymo. He countered that his actions would hasten the development of self-driving cars. The court's eventual ruling was that indeed, Uber had used the stolen trade secrets, and Levandowski was sentenced to prison for theft.
These cases add weight to the fine balance between proprietary control and public access to information. With one eye on the widely accepted view that organizations have a right to protect their intellectual property, consumers also have rights of access and use for content legally obtained. The DeCSS and Waymo vs. Uber cases underpin, in their own way, the debate about how far proprietary rights should be propagated and what level of public access should be given.

The more general ramifications of this tension between proprietary control and public access are considerable. In a digitized era, access to and the spread of information is ever more important for individuals, businesses, and society generally. Proprietary control over information can limit access, stifle innovation, and exaberate existing inequalities.

On the other hand, free access to information raises concerns regarding privacy, intellectual property rights, and misuse. There are some pretty complicated trade-offs at issue, with the tough ethical, legal, and economic considerations.

This, then, lays the foundation for the raging debate over the dichotomy of proprietary control versus public access. Governments, businesses, and individuals must stay tuned to develop policies and practices that will promote both innovation and fairness.