Activity 01

CST 497-2
Social, Ethical and Professional Issues in Computing

CST/20/034
RFR.BEGUM

Computer Science and Technology
Department of Computer Science and Informatics
Faculty of Applied Sciences
Uva Wellassa University of Sri Lanka

The following 20 real-world computing incidents that present significant ethical dilemmas. Each
case can spark discussion around professional responsibility, privacy, fairness, and the potential
social impact of technology.
You are required to evaluate each case and provide your insights considering its professional
responsibility, privacy, fairness, and the potential social impact of technology.

1. Cambridge Analytica and Facebook Data Scandal
* Dilemma: The use of personal data from millions of Facebook users without their consent to influence political campaigns.
* Ethical Question: Is it ethical to use data for purposes users are unaware of?

- **Professional Responsibility**
  - Issue: Cambridge Analytica harvested the personal data of millions of Facebook users without their consent and used it to influence political campaigns.
  - Insight: Companies handling personal data must ensure transparency in its use. Professionals in tech must advocate for data use policies that respect user consent.

- **Privacy**
  - **Issue**: Facebook users' private data was accessed and used without consent for political targeting.
  - Insight: Privacy violations undermine user trust. Clear consent and user control over personal data must be a priority for all digital platforms.

- **Fairness**
  - **Issue**: Users were unfairly subjected to manipulation in political campaigns based on unauthorized data use.
  - **Insight:** Systems should treat all users fairly by ensuring that no individual or group is unfairly targeted based on harvested data.

- **Social Impact**
  - **Issue:** The scandal fueled distrust in social media platforms and increased scrutiny over data use in politics.

- **Insight**: Public awareness and demand for stronger data protection laws grew as a result of the scandal.

2. AI Bias in Hiring Algorithms

* Dilemma: AI algorithms used in hiring by companies like Amazon were found to be
biassed against women.
* Ethical Question: How do we ensure fairness in AI decision-making?

- **- Professional Responsibility**

- **Issue**: AI algorithms used in hiring, such as Amazon's, were found to be biassed against women.

- **Insight**: Developers of AI systems must ensure fairness by eliminating bias in training data and algorithmic processes.

- Privacy

- **Issue**: The data used in AI hiring systems may contain private information that is not relevant to job performance.

- **Insight**; Companies must ensure AI systems do not rely on private, irrelevant data when making hiring decisions.

- Fairness

- **Issue**: AI systems discriminated against female applicants, resulting in an unfair hiring process.

- **Insight**: Fairness requires that all candidates are evaluated equally, without bias based on gender, race, or other irrelevant factors.

- **Social Impact**

- **Issue**: Biassed AI systems exacerbate existing inequalities in employment.

- **Insight**: The use of biassed AI in hiring could widen the gender and racial wage gaps, harming long-term societal equity.

3. Apple vs. FBI Encryption Dispute

* Dilemma: The FBI requested Apple to unlock an iPhone used by a terrorist, but Apple
refused due to user privacy concerns.
* Ethical Question: Should privacy or national security take precedence?

- **Professional Responsibility**

- Issue: Apple refused to unlock a terrorist's iPhone, citing concerns over user privacy.

- Insight: Companies like Apple must balance ethical responsibility between protecting user privacy and complying with law enforcement requests.

- **Privacy**

- Issue: Unlocking the iPhone could compromise the privacy of all iPhone users.

- Insight: Privacy is paramount in the digital age, but there may be situations where limited access is justified for national security.

- **Fairness**

- Issue: The balance between privacy and national security is difficult to maintain, especially when lives are at risk.

- Insight: Fair policies must address how privacy can be respected without impeding critical law enforcement efforts.

- **Social Impact**

- Issue: The case intensified the debate over privacy vs. security.

- Insight: This conflict affects public trust in tech companies, as users want to ensure their data is safe from both hackers and unwarranted government access.

4. Self-Driving Car Fatalities (Uber/Waymo)

* Dilemma: Autonomous vehicles have been involved in fatal accidents during testing.
* Ethical Question: Who is responsible for decisions made by AI in life-or-death situations?

- **Professional Responsibility**

- Issue: Self-driving cars have been involved in fatal accidents during testing.

- Insight: Engineers and companies must take responsibility for ensuring autonomous vehicles undergo thorough safety testing before widespread deployment.

- **Privacy**

- Issue: Autonomous vehicles collect massive amounts of data on user behaviour and location.

- Insight: While improving safety, the data collection practices of these cars must respect privacy rights.

- **Fairness**

- Issue: Fatal accidents disproportionately impact pedestrians or other road users who are not involved in the decision to use such technology.

- **Insight**: The fairness of autonomous vehicle testing must take into account the rights of all affected individuals, not just the passengers.

- **Social Impact**

- Issue: Public trust in AI-powered vehicles is undermined by fatal incidents.

- Insights: Long-term adoption of autonomous vehicles depends on public perception of their safety and societal benefits.

5. Google's Project Maven

* Dilemma: Google worked with the Pentagon on AI to analyze drone footage, leading to
internal protests over ethical concerns.
* Ethical Question: Should tech companies be involved in military applications of AI?

- **Professional Responsibility**

- Issue: Google's involvement in a military project using AI to analyze drone footage sparked ethical concerns.

- Insight: Tech companies must critically evaluate the implications of their products being used in military applications, balancing profit with ethical considerations.

- **Privacy**

- Issue: Military surveillance using AI raises concerns over privacy in conflict zones.

- Insight: AI surveillance must be carefully regulated to avoid infringing on individuals' rights, even in military settings.

- **Fairness**

-Issue: The use of AI in warfare raises questions about fairness in targeting and decision-making.

- Insight: Fair use of AI in military contexts requires strict oversight to prevent misuse and discrimination.

- **Social Impact**

- Issue: Internal protests among Google employees highlighted the societal concern over the role of AI in warfare.

- **Insights:** Public debate on the use of AI in military operations could shape future policies on tech company involvement in defense contracts.

6. Facial Recognition and Privacy Violations (Clearview AI)

* Dilemma: Clearview AI scraped billions of images from the internet to develop facial
recognition tools for law enforcement.
* Ethical Question: Is it ethical to use public images without consent for surveillance?

- **Professional Responsibility**

- Issue: Clearview AI scraped billions of images from the internet to develop facial recognition tools for law enforcement, without consent.

- **Insight:** Companies using facial recognition must prioritize user consent and limit data collection to lawful, transparent purposes.

- **Privacy**

- Issue: Using public images without consent for surveillance purposes is a severe invasion of privacy.

- **Insight:** Privacy in the digital age includes control over how publicly available information is used, especially in surveillance.

- **Fairness**

- **Issue**: Facial recognition technology is often biassed and inaccurate, leading to unfair targeting of minorities.
- **Insight:** Fairness demands that facial recognition systems be thoroughly tested and free from bias before being implemented in law enforcement.

- **Social Impact**

- **Issue:** The widespread use of facial recognition by law enforcement has led to concerns over surveillance states.
- **Insight:** Public mistrust in facial recognition can lead to protests and calls for stronger regulation of AI technologies in policing.

7. The Right to Be Forgotten (Google vs. EU)

* Dilemma: The EU Court of Justice ruled that individuals have the right to request
removal of personal data from search engines.
* Ethical Question: Should people have control over erasing their digital footprints?

- **Professional Responsibility**

- **Issue:** The EU ruled that individuals have the right to request removal of personal data from search engines.
- **Insight:** Search engines must balance the right to information with the right to privacy, ensuring ethical use of personal data.

- **Privacy**

- **Issue:** The right to be forgotten gives individuals control over their digital footprint.
- **Insight**: Privacy concerns must allow individuals to remove outdated or harmful information from public view.

- **Fairness**

- **Issue**: Not all information requests are equally justified, and balancing public interest with personal privacy can be challenging.

- Insight: Fairness requires search engines to develop clear, consistent policies on which data can be removed and which should remain accessible.

- **Social Impact**

- Issue: This ruling has a significant socil impact, particularly regarding freedom of speech and access to historical records.

- Insight: The debate over privacy vs. public access to information could shape future laws on digital content management.

8. Social Media Misinformation (COVID-19, Elections)

* Dilemma: The spread of misinformation about COVID-19 and elections on platforms like
Twitter, Facebook, and YouTube.
* Ethical Question: Should social media companies be held accountable for the spread of
Misinformation?

- **Professional Responsibility**

- Issue: Platforms like Twitter, Facebook, and YouTube allowed misinformation about COVID-19 and elections to spread.

- Insight: Social media platforms have a responsibility to moderate content that can harm public health or democracy.

- **Privacy**

- Issue: The algorithms that control content distribution often use private user data to target misinformation.

- Insight: Platforms must ensure that privacy is respected even as they fight misinformation, avoiding intrusive data collection.

- **Fairness**

- Issue: The spread of misinformation can disproportionately harm certain groups, such as vulnerable populations with limited access to factual information.

- Insight: Fairness requires that all users receive accurate, verified information to make informed decisions, especially on critical issues.

- **Social Impact**

- Issue: Misinformation on social media has had serious consequences, from public health crises to undermining democratic processes.

- Insight: The social responsibility of tech platforms to prevent misinformation is a growing area of concern, influencing public policy and regulation.

9. Tesla Autopilot Crashes

* Dilemma: Tesla's autopilot system has been involved in crashes, raising questions about
safety and human reliance on AI.
* Ethical Question: How do we balance the risks and benefits of semi-autonomous
Technology?

- **Professional Responsibility**

- Issue: Tesla's autopilot system has been involved in crashes, raising questions about safety and reliance on semi-autonomous technology.

- Insight: Companies must rigorously test semi-autonomous systems and provide clear user guidelines to prevent overreliance on technology. Developers and manufacturers are responsible for ensuring that these systems function safely in real-world conditions, and they must clearly communicate the limitations of the technology to users. Continuous updates and improvements should be part of the company's commitment to public safety.

- **Privacy**

- Issue: Tesla collects data from its vehicles to improve the performance of its autopilot system.

- Insight: Although data collection helps enhance the technology, privacy concerns arise if user consent and transparency are not prioritised. Tesla must ensure that personal driving data is securely stored, anonymized where appropriate, and used only with the driver's informed consent.

- **Fairness**

- Issue: Semi-autonomous systems may be marketed as safer than they truly are, leading some drivers to overestimate their capabilities.

- Insight:Fairness requires that users be accurately informed about the capabilities and risks of autopilot features. Marketing should not mislead customers into thinking the technology is fully autonomous or capable of handling all driving situations, ensuring a fair understanding of the product's limitations.

- **Social Impact**

- Issue: Crashes involving autopilot systems can decrease public trust in autonomous driving technology and slow adoption.

- Insight: Tesla and other manufacturers play a key role in shaping the future of autonomous vehicles. The social impact of crashes involving autopilot systems includes heightened public scepticism, which can hinder technological progress. To foster trust, manufacturers must demonstrate a commitment to safety, transparency, and accountability.

10. Big Data and Predictive Policing (COMPAS)

* Dilemma: Predictive policing algorithms, such as COMPAS, were found to disproportionately target minority communities.
* Ethical Question: How do we prevent discrimination in data-driven policing?

- **Professional Responsibility**

- Issue: Predictive policing algorithms like COMPAS disproportionately target minority communities.

- Insight: Developers and law enforcement must ensure that data-driven systems do not perpetuate or exacerbate systemic biases.

- **Privacy**

- Issue: Predictive policing systems rely on vast amounts of personal data.

- Insight: Privacy concerns arise as such systems often use personal information without explicit consent, which can lead to surveillance-like practices.

- **Fairness**

- Issue: These systems unfairly target minorities and reinforce racial profiling.

- Insight: Fairness demands that predictive systems be designed to minimise bias and offer equal treatment regardless of race or background.

- **Social Impact**

- Issue: Predictive policing can erode trust in law enforcement, especially among marginalised communities.

- Insight: The use of biassed systems can deepen societal inequalities and foster resentment, leading to social unrest.

11. Google Street View Data Collection

* Dilemma: Google's Street View cars accidentally collected private data from Wi-Fi
networks while mapping cities.
* Ethical Question: How should companies handle accidental data collection?

- **Professional Responsibility**

- Issue: Google's Street View cars accidentally collected private data from Wi-Fi networks.

- Insight: Tech companies must establish clear policies and protocols to handle data responsibly and ensure it is not collected or used without consent.

- **Privacy**

- Issue: Google's unintended collection of private Wi-Fi data breached user privacy

- Insight: Even if data collection is accidental, companies must take steps to delete and protect private information immediately.

- **Fairness**

- Issue: Users whose private data was collected were unaware and unable to consent.

- Insight: Fairness dictates that users be informed and allowed to control what data is collected about them.

- **Social Impact**

- Issue: Incidents like this reduce public trust in tech companies and their handling of personal data.

- Insight: This breach highlighted the need for stricter regulations on corporate data collection practices.

12. Therac-25 Radiation Machine Incident

* Dilemma: A software error in the Therac-25 radiation machine led to fatal overdoses of
radiation.
* Ethical Question: What responsibility do software engineers have for ensuring the safety
of critical systems?

- **Professional Responsibility**

- Issue: A software error in the Therac-25 radiation machine led to fatal overdoses of radiation.

- Insight: Engineers and companies must take responsibility for ensuring the safety and reliability of critical healthcare technology.

- **Privacy**

- Issue: The failure did not directly affect privacy but involved medical data and treatment plans.

- Insight: Medical technology must protect patient data and prevent life-threatening errors from occurring.

- **Fairness**

- Issue: Patients receiving faulty treatment suffered unjust harm.

- Insight: All patients deserve access to safe, reliable healthcare technology. Companies must ensure that such technology undergoes rigorous testing before deployment.

- **Social Impact**

- Issue: The malfunctioning of a medical device harmed the reputation of technological advances in healthcare.

- Insights: This incident prompted industry-wide reform in medical technology standards and software safety testing.

13. TikTok and Data Privacy Concerns

* Dilemma: Concerns over TikTok's collection and storage of user data by its parent
company in China.
* Ethical Question: How should companies handle user data when national security is at
stake?

- **Professional Responsibility**

- Issue: Concerns were raised about TikTok's collection and storage of user data by its parent company in China.

- Insight: Social media companies must be transparent about where and how user data is stored, particularly in cases involving international entities.

- **Privacy**

- Issue: Users were concerned about TikTok's collection of personal data, particularly in light of its potential access by foreign governments.

- Insight: User privacy must be prioritised, with clear boundaries around what data is collected and who can access it.

- **Fairness**

- Issue: Data collection practices were not made clear to users, leading to unequal understanding of privacy risks.

- Insight: Fairness requires that all users be fully informed about how their data is being used and the potential risks involved.

- **Social Impact**

- Issue: The privacy concerns surrounding TikTok sparked debates over national security and global data flows.

- Insight: This controversy has influenced the broader debate on tech companies' role in international data sharing and national security.

14. Amazon Ring and Police Partnerships

* Dilemma: Amazon Ring shared footage from home security cameras with law enforcement, raising privacy concerns.
* Ethical Question: Should private companies cooperate with law enforcement without user
consent

- **Professional Responsibility**

- Issue: Amazon Ring shared footage from home security cameras with law enforcement without clear user consent.

- Insight: Companies offering surveillance technology must protect user autonomy and prevent unauthorised data sharing with third parties, including law enforcement.

- **Privacy**

- Issue: Ring users' footage was shared with law enforcement without their explicit knowledge or permission.

- Insight: Privacy is compromised when user-generated data is shared with external organisations without consent.

- **Fairness**

- Issue: Not all users were aware that their data could be shared with police, leading to potential overreach.

- Insight: Fairness demands that users have full control over how their surveillance data is used.

- **Social Impact**

-Issue: The partnership between Amazon and law enforcement raised concerns about the increasing surveillance of public and private spaces.

- Insight: Public debate has shifted toward the balance between safety and personal privacy in an era of widespread surveillance technology.

15. Facebook Algorithm and Hate Speech Amplification

* Dilemma: Facebook's algorithms have been criticised for amplifying hate speech and
polarising content for engagement.
* Ethical Question: Should platforms prioritise engagement over ethical responsibility?

- **Professional Responsibility**

- Issue: Facebook's algorithms were found to amplify hate speech and polarising content in an effort to increase user engagement.

- Insight: Social media platforms must take responsibility for ensuring that their algorithms promote healthy discourse, rather than prioritizing engagement over ethics.

- **Privacy**

- Issue: Facebook uses personal data to tailor and push inflammatory content to users.

- Insight: The use of private data to manipulate user experiences and amplify divisive content raises significant privacy concerns.

- **Fairness**

- Issue: Users are exposed to content that may promote hate or discrimination based on algorithmic biases.

- Insight: Fairness requires that platforms avoid favouring content that fosters division, and instead promote inclusive and respectful discussions.

- **Social Impact**

- Issue: The amplification of hate speech has fueled political polarization and real-world violence in various regions.

- Insight: This problem has led to global calls for social media regulation, especially regarding content moderation and algorithm transparency.

16. Software Piracy in Developing Countries

* Dilemma: Widespread use of pirated software in developing countries due to high costs
of legal versions.

* Ethical Question: Is it ethical to enforce strict copyright laws when access is limited by
cost?

- **Professional Responsibility**

- Issue: The widespread use of pirated software in developing countries due to high costs of legal versions.

- Insights: Tech companies need to develop more affordable, accessible alternatives to help combat piracy while providing fair access to software.

- **Privacy**

- Issue: Pirated software can pose security risks, as it often lacks updates and can contain malware that compromises user privacy.

- Insight: Users may not be aware of the privacy risks posed by pirated software, highlighting the need for more affordable legal alternatives.

- **Fairness**

- Issue: People in developing countries often resort to pirated software due to prohibitive costs, creating inequitable access to technology.

- Insight: Fairness requires that software companies offer pricing models that accommodate users in various economic conditions.

- **Social Impact**

- Issue: Piracy undermines local software development and can negatively affect the global software market.

- Insight: Creating equitable access to software may promote innovation and reduce piracy rates, benefiting both users and the software industry.

17. Amazon Mechanical Turk and Worker Exploitation

* Dilemma: Amazon's Mechanical Turk platform offers micro-tasks for minimal pay,
raising concerns about labour exploitation.
* Ethical Question: Should tech platforms ensure fair pay for gig workers?

- Professional Responsibility

- Issue: Amazon's Mechanical Turk platform offers micro-tasks for minimal pay, raising concerns about labour exploitation.

- Insight: Tech platforms must ensure fair treatment and compensation for gig workers, especially in terms of wage standards and working conditions.

- **Privacy**

- Issue: Workers often disclose personal information when completing tasks for low pay.

- Insight: Platforms must respect workers' privacy and ensure that they are not being exploited for cheap labor while compromising their personal information.

- **Fairness**

- Issue: Workers, many from developing countries, are often underpaid and overworked.

- Insight: Fairness demands that companies ensure fair wages and ethical working conditions for all gig workers, regardless of location.

- **Social Impact**

- Issue: The exploitation of gig workers raises larger questions about the future of labor and the gig economy.

- Insight: The low wages and poor working conditions on platforms like Mechanical Turk have sparked broader debates about labor rights in the digital age.

18. Deepfake Technology

- **Professional Responsibility**

- Issue: Deepfakes are increasingly being used for unethical purposes, such as fake news or revenge porn.

- Insight: Developers of deepfake technology must create safeguards to prevent its misuse and promote responsible use of the technology.

- **Privacy**

- Issue: Deepfakes can be used to impersonate individuals without their consent, violating their privacy and reputation.

- Insight: Strong privacy protections are needed to ensure individuals' identities are not manipulated without their consent.

- **Fairness**

- Issue: The use of deepfakes can unfairly damage reputations or mislead the public.

- Insight: Fairness requires that any use of this technology be carefully regulated to prevent

19. Theranos Blood Testing Fraud

- **Professional Responsibility**

- Issue: Theranos falsely claimed that its technology could run comprehensive tests from a single drop of blood. This misrepresentation was deceptive and put patients at risk. The company's leadership, including founder Elizabeth Holmes, failed in their duty to provide accurate information and ensure the safety and reliability of the medical device.

- Insight: In the healthcare industry, professionals are bound by strict ethical standards to ensure that medical technologies are rigorously tested and validated before reaching the market. A breach of this responsibility can have life-threatening consequences for patients. Companies must prioritise the well-being of users over profit or growth.

- **Privacy**

- Issue: While the primary focus in this case isn't the misuse of personal data, the fraudulence of the technology indirectly affects patient privacy. Patients trusted Theranos with their health data and their blood samples, believing they were receiving accurate diagnostics.

- Insight: Maintaining patient trust is a key aspect of privacy in healthcare. When companies deceive patients, they not only breach professional ethics but also damage the implicit trust that patients place in healthcare providers to handle their personal health data responsibly.

- **Fairness**

- Issue: The fraudulent claims led patients, investors, and healthcare professionals to make decisions based on false information. Patients were unfairly subjected to incorrect medical results, which could lead to harmful treatments or lack of necessary care.

- Insight: Fairness in healthcare hinges on transparency and honesty. Technologies must be tested and validated to ensure that patients of all backgrounds receive accurate and safe medical care. Misleading practices disproportionately affect vulnerable individuals who might not have the resources to seek second opinions or alternative treatments.

- **Social Impact**

- Issue: The scandal shook public confidence in healthcare startups and innovation in medical technology. It created a ripple effect of skepticism around new medical technologies, especially those claiming revolutionary advances.

- Insight: The collapse of Theranos had a lasting social impact, increasing public scrutiny of health tech companies and regulatory bodies. It also highlighted the need for more stringent oversight in the development and deployment of medical technologies to prevent harm to the public.

20. Data Breaches and Security (Equifax, Marriott)

- **Professional Responsibility**

- Issue: Equifax and Marriott, two major corporations, suffered massive data breaches that exposed the personal information of millions of customers. These breaches highlighted the companies' failure to uphold their professional responsibility to protect sensitive user data. The inadequate cybersecurity measures employed by both companies allowed hackers to infiltrate their systems, leading to massive data theft.

- Insight: Organisations that handle personal information have a professional obligation to implement robust security measures. This includes regular audits, prompt security updates, and comprehensive encryption of sensitive data. Negligence in this area represents a clear breach of responsibility, and companies must invest in cybersecurity to prevent such incidents.

- **Privacy**

- Issue: The data breaches compromised the privacy of millions of people, exposing sensitive details like Social Security numbers, credit card information, and personal addresses. The victims had little recourse after their data was stolen, leaving them vulnerable to identity theft and fraud.

- Insight: In a digital world, privacy is a fundamental right that must be respected by corporations. Companies are custodians of user data and must implement the highest standards of privacy protection. Users have a reasonable expectation that their personal information will be handled securely and that any breaches of trust will be swiftly addressed.

- **Fairness**

- Issue: The data breaches did not impact all customers equally. Those who could afford credit monitoring services or legal recourse were in a better position to recover from the consequences of the breach. Meanwhile, those from lower socioeconomic backgrounds may have been disproportionately affected by the financial and personal fallout.

- Insight: Fairness dictates that all users, regardless of their financial status, should be protected equally from data breaches. Companies must ensure that they have proactive systems in place to address these concerns and offer support to all customers, especially those who may not have the resources to mitigate the effects of data theft.

- **Social Impact**

- Issue: The widespread data breaches led to public distrust in large corporations and their ability to protect personal information. Many individuals

faced long-term consequences, such as credit fraud and identity theft, because their personal information was exposed.

-Insight: The social impact of these breaches extends far beyond the immediate financial damage. They have altered how individuals engage with digital services and companies. As a result, there is increased demand for stricter regulations around data privacy, with a push for harsher penalties for companies that fail to protect user .