Software Engineer

Caitlyn Cook

General Instructions

1. For each page, synthesize the reading and research by writing in complete sentences in essay format.
   a. Use the green instructions in the notes below each page to focus your research and writing.
   b. Write about each question, prompt, or process provided in those notes.
   c. Write a full page of text with lots of detail (about 250 words).
   i. Don’t generalize so much that your writing is devoid of detail.
   ii. Don’t repeat yourself.
   d. Cite each source by adding a hyperlink in the Title of the Article or law.
   e. Do not change the template:
      i. Text must be 14 point Lato left-justified type.
      ii. Refrain from adding extra margins or double spacing.
      iii. Do not bullet the paragraphs. Write in essay format only.
   f. Add additional pages if you need more room.

2. Add all sources to the Bibliography page.
   a. Include author, year, title, publisher, and URL.
   b. Number or bullet them using the list button.

When in doubt, write to the instructor for clarification using the Canvas Inbox.
Although immediately after graduation, I have accepted a job as a Software Developer for HP, Inc, I will choose to focus on my future career goals for this assignment. For this assignment, I have located a job posting for a Data Scientist at Facebook. In the posting, Facebook describes their company goals of building community and connecting people. This job posting is recruiting someone to work with data relating to Facebook’s core products (“Instagram, Messaging, Growth, Engagement, Ads” as described in the posting). The main responsibilities of the role are quantitative analysis of the extremely large amounts of data that Facebook has access to, in order to generate insights and new information that can guide the development and improvement of existing or new Facebook products. Specifically, the posting describes four categories of work: product operations, exploratory analysis, product leadership, and data infrastructure. Product operations involves generating and evaluating metrics and experimental results to set goals and guide the development of Facebook’s products. Exploratory analysis involves looking into the future, identifying long term trends and generating ideas for future products. Product leadership involves guiding development by making recommendations, communicating results, and creating “best practices” for teams. Data infrastructure involves working with Facebook’s databases and data sources, improving the process of ingesting new data and maintaining the existing stored data. This role does not require any specific exams, certifications, or union memberships beyond a bachelor’s degree in a technical field, although advanced degrees are preferred. It also requires 2 years of experience with quantitative analysis.
I am working on Facebook’s data gathering and ingesting process, working to improve the quality and usability of the data. While I am working, I notice a vulnerability in the data transmission process that exposes unencrypted user data to the public through the process of sending it to Facebook’s internal storage. It is only a small part of the process, but some of the information could be personally identifying. In this dilemma, clause 1.6 Respect privacy applies, as well as 1.7 Honor confidentiality. 1.6 counsels professionals to ensure that personal data is being used for legitimate purposes, that users are properly informed of its gathering, and that users have the ability to delete or correct their data if desired. It also involves the security of the data, preserving anonymity when necessary and preventing unauthorized access. 1.7 counsels professionals not to disclose sensitive information except where legally or ethically necessary.

The first action I could take to solve the problem is to attempt to find a technical solution to the breach myself. If it were a system I was familiar with, or perhaps had a hand in designing, it is possible that I may understand the problem and technical environment enough to solve the problem. The second action I could take would be to inform my team and superiors, so that Facebook could initiate the relevant processes to seal the breach, inform users, and take any legal action necessary. The third action I could take, which may be required if Facebook chose not to take action, would be to inform the public of the potential breach by reaching out to news media.
Hardware Dilemma

Over the course of my work, I overhear about Facebook’s new project, the Portal. Described here in “Facebook tries its hand at hardware with Portal” for TechCrunch, the Portal is a dedicated video-calling device that can automatically track users as they move around, moving the camera and adjusting the zoom as necessary. From discussions with other employees working on the project, it sounds like Facebook isn’t being very careful with their supply chain to manufacture the devices, and could be using materials that come from unethical sources. Not all the companies they are purchasing materials from are known to be child labor free, and some are known to have very poor treatment of their workers. In this case, 1.2 Avoid harm applies, as well as 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks. The manufacturing process and supply chain could be causing harm to its workers if they are in poor conditions, and in developing this device, Facebook increases the demand for such harmful practices.

In this case, the first action I could take would be to meet with those working on or overseeing the project to express my concerns, and ask about their plan for preventing these issues. A second action I could take, if conversations confirm the problem, is to organize protest among the employees of the project, aiming to pause work on it until the ethical nature of the manufacturing can be improved. A third action I could take would be to attempt to publicize the problems with the device, to discourage consumer demand in an attempt to pressure Facebook to improve conditions.
Advertising, Search, or News Dilemma

Facebook is famous for its difficulties with fake news, incomplete or sensationalist information, and content bias enforced by echo chambers or ideological bubbles. Imagine I am studying engagement with user posts, both of individual personal accounts and company or organizational pages. I find that sensationalist content generates higher levels of engagement, especially when related to current political topics. I find that many media pages are taking advantage of this, exaggerating or falsifying information to drive up their engagement. In this scenario, clause 1.3 Be honest and trustworthy applies. The spreading of false or exaggerated information is dishonest, and Facebook should not be encouraging the spread of incorrect or inflammatory information by rewarding it with better metrics.

In this case, as a data scientist at Facebook I would be uniquely situated to attempt to solve this problem. While it is a complex problem that will not likely be solved by a single action, my first action would be to highlight it as an interesting and useful trend to the teams that I work with, to engage them with the problem and allow it to guide their work as well. A second action I could take would be to conduct experiments on user engagement with these and other posts, to determine if there are ways to encourage engagement with more truthful posts, or discourage engagement with dishonest posts. A third action I could take would be to implement a system that identifies posts which may contain charged language, which could be used to warn users or to take action against pages that regularly post such content.
I am investigating uses of Facebook’s features when I come across a group using the site to organize protests against conditions in their local area. The page has an unusually high amount of content reported by users as in violation of Facebook’s policies, and some, but not all, of the reported content is actually in violation. Some of the content could be interpreted as inciting violence, although much of it is acceptable. In this scenario, 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing applies, as well as 1.2 Avoid harm.

The protestors are using the site to attempt to improve their conditions, which contributes to human well-being, and as users of the site they are stakeholders in its policies and disciplinary actions. Since the conditions they are protesting may be causing them harm, I may need to be careful not to enable or encourage that harm if I take action.

The first action I could take would be to issue disciplinary action against the specific users that have posted terms violating content, perhaps a temporary ban from posting content or from logging in to the site. Another action could be to institute a stricter moderation policy on the group, requiring posts to be approved by a human before they are published, so that questionable content is easier to catch. A third action would be to take disciplinary action against those who make false reports against the page, reporting valid content in an attempt to get it removed, or get the page taken down.
I am investigating the content of Facebook posts by some pages, and I uncover a trend of posting stolen, private, or otherwise unauthorized content. The content consists of copyrighted artwork, photographs, videos, writing, or other intellectual property that is protected by copyright laws. Often, no credit is given, or it is impossible to trace back the content to its creator. In this case, 1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts applies, as well as 2.8 Access computing and communication resources only when authorized or when compelled by the public good by some interpretation. The content was created by individuals who deserve to benefit from it, rather than have those benefits claimed by another person. Although I myself, or Facebook as a company or service, is not directly accessing the copyrighted content, we are facilitating and rewarding the unauthorized access.

In this case, one action I could take would be to suggest the creation of some form of media ownership tracking for posts. Users could have the option to tag an owner in their post in order to credit them, passing most or all of the benefits from the post to the creator. They could also have the option to claim that a post contains their content. A second action could be to develop a partnership with Google’s reverse image search to develop a system that flags potentially stolen content. A third action could be to investigate ways to promote understanding of and engagement with Facebook’s current takedown policies.
Whistleblowing

Of those described, the scenario most likely to necessitate whistleblowing is the Software Dilemma, in which a large amount of potentially personally identifying information is accidentally leaked. From reading the listed agencies, the most appropriate place to report seems to be the Computer Emergency Readiness Team, reporting the vulnerability in the pipeline. Their Vulnerability Disclosure Policy instructs persons to send an email (preferably encrypted) or make a phone call to the provided contact information. Following the report, they will reach out to the vendor and attempt to determine a plan and timeline for fixing the issue and disclosing the vulnerability to the public. Many factors affect this timeline, including severity of the threat, difficulty of mitigation, vendor responsiveness, and previous public disclosure affect this timeline. Unless the person filing a report specifically requests anonymity, their name and contact information will be provided to the vendor about which they make the report. During the process of resolving the vulnerability, the CISA team will provide updates to the vulnerability reporter, as long as doing so does not reveal the vendor’s private information. If a vendor does not respond to CISA inquiries, or is uncooperative once contact has been made, CISA “may disclose vulnerabilities as early as 45 days after the initial attempt to contact the vendor is made, regardless of the existence or availability of patches or workarounds”. The official process contains five steps - detection and collection, analysis and detailed examination of the issue, mitigation coordination and development, application of mitigation, and disclosure.
Ethical theory/approach governing my decision making

Throughout most of these dilemmas, my ethical decision making has been guided by the rights approach, described here in “A Framework for Ethical Decision Making” by the Markkula Center for Applied Ethics. A large company like Facebook that provides a service that is so integral to the daily social, professional and personal lives of many people must be very careful to respect the rights of all those involved. I believe that using the rights approach is a good choice because many rights are clearly spelled out, through legislation, previous legal decisions, or even the rights described in the UN’s Universal Declaration of Human Rights. The clarity and specificity of these guidelines are helpful when balancing the wants and needs of so many different groups of people, some of which may conflict with each other. It also allows the company to have a clear and easily defensible justification for their actions. This is valuable, because there is no shortage of people, organizations, and governments ready and eager to criticize the actions of major corporations. This criticism is a valid and useful part of ethical and societal discourse, but it must not prevent or discourage companies from taking ethical action for fear of appearances. The rights approach also gives explicit protection to historically marginalized or disenfranchised groups, which have often been denied their rights or had their rights disrespected. An explicit focus on those rights provides a space with equal rights for all involved, creating a level playing field and allowing opportunities for disenfranchised groups to exercise power.

“Question: Is it ethical (or even legal) for a company to prosecute an individual for discovering a vulnerability when they purposely broke in, grey-hat style, but they caused no harm?”, 2019. Association for Computing Machinery. https://ethics.acm.org/integrity-project/ask-an-ethicist/ask-an-ethicist-grey-hat-hacking/


Bibliography