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.
The responsibilities of a software engineer at Mozilla are detailed in the Mozilla job listing DOM editor, Software Engineer. The main responsibilities include working with a team of engineers to address problems with and improve the Firefox web browser's rendering engine. This involves technical aspects such as hardware utilization to more human sided aspects such as the experience of users who speak languages other than english.

The position requires an applicant with experience in developing and debugging concurrent C++ code and modern web technologies. The listing emphasizes ability to work with others and interest in learning about new and existing technologies as equally important to technical knowledge. Logically, one could assume that a degree in a computer science related field is required, but no specific degree requirements are listed. Additionally, no related experience is present as a requirement on the job listing.

All Mozilla employees adhere to Mozilla Community Participation Guidelines. This is a code of conduct is a requirement for anyone who for or with Mozilla as well as those who participate in any of their events. The goal of the participation guidelines is to establish an environment where everyone can thrive regardless of their background or orientations. They apply at any of Mozilla's office spaces as well as any public Mozilla events or offsite training. The guidelines emphasize being respectful and inclusive while still being direct with disagreements when applicable. As in life, conflict is inevitable in the workplace. Adherence to the community participation guidelines means dealing with conflict in a way that is both professional and respectful. Violations of the guidelines will result in a variety of consequences including termination of employment.
According to cybersecurity company Norton, browser hijacking is the process of a piece of software accessing or editing a browser’s settings without the knowledge or consent of the user. In their article What Are Browser Hijackers?, it is stated that the most common goal of browser hijacking is to reroute traffic to unwanted web pages. Additionally, spyware and other malicious programs can also be installed in order to steal user credentials.

In ensuring that user credentials such as bank logins remain private, web browser developers must adhere to the ACM Code of Ethics section 1.2 Avoid Harm. The overarching idea behind avoiding harm is to avoid any negative consequences. In the context of web browsers developers should take all necessary steps to avoid any unwanted access of user data. The process of preventing browser hijacking is complex. The methods that cybercriminals use to steal user information are constantly evolving. As security holes are addressed, new ways to commit computer crime emerge. This means that as a browser developer, the main action I could take to address the problem of browser hijacking is to constantly strive to improve the security of the application. As new security flaws arise they should be taken care of as quickly as possible. As Norton points out in their article mentioned above, browser hijacking can also come from seemingly trustworthy sources such as browser add-ons. A system for reporting such behavior from add-ons and disabling them should be in place. A last action that I could take is to listen to user feedback on security issues and take action accordingly. As Frank Schroeder discusses in the article Why is User Feedback Important For Software Development?, listening to user feedback improves the developers ability to locate and fix problems in their software.
The Environmental Protection Agency states that electronic waste is a general term for scrap electronics that have reached the end of their useful lives in their article *Cleaning Up Electronic Waste*. Properly recycling electronic waste is important because of the potential for the toxic elements that electronics are often composed of to leak into the environment. In ensuring that unused electronics are disposed of properly at electronic waste recycling centers, ACM Code of Ethics section 1.2 Avoid Harm is subscribed to by addressing and avoiding the negative consequences of harmful toxins seeping into natural areas.

One way that a software developer can indirectly address the problem of electronic waste is to design programs so that they can run efficiently on old hardware. As Ed Sperling discusses in the article *Making Software More Efficient* there are several benefits to striving for efficiency in software development. In addition to running more efficiently on older hardware, efficient applications save power and provide a faster user experience. While this extends the useful life of electronics, the reality is that all electronics will eventually become obsolete. Software companies can sponsor programs to recycle old hardware. Companies such as LG and Sony have already begun programs similar to this as outlined in the article *Recyclers, Tech Companies Step Up E-Waste Standards*. In addition to sponsoring recycling programs, information can be provided to clients on how to properly recycle old devices. Samsung provides exactly this service on their page *What is Samsung Recycling Program*. The page offers information on why recycling electronics is important and how it can be done. While electronic waste will likely always exist, programs that inform the public on the importance of recycling help to mitigate the problem.
Advertising, Search, or News Dilemma

In the paper De-Identified Data and Third Party Data Mining: The Risk of Re-Identification of Personal Information written by Christine Porter, the importance of anonymizing data before allowing analysis by third parties is discussed. Matching seemingly anonymous participants in a set of data can often be an easy task. Collecting information about user experiences in order to analyze it in hopes of improving a service is a common practice. In making sure that no identifying information is turned over to third parties organizations align with the ACM Code of Ethics sections 1.6 Respect Privacy and 1.7 Honor Confidentiality.

One way that I could address the issue of identifying information being accidentally included in datasets that are mined by third parties as a software developer is to not allow any data mining of such datasets. If a dataset does not include any information about user information then no users are at risk of being identified by it. Another way is to allow users to opt out of participating. As discussed by Annalee Newitz in the article Dangerous Terms: A User’s Guide to EULAs, user agreements can often include terms that are harmful to customers. These situations can be avoided by allowing users to simply reject a user agreement that allows for third party mining of their data. A last strategy for avoiding user privacy issues when allowing third parties access to their data is to only allow reputable and trustworthy companies access. As detailed in Zoe Kleinmann’s BBC article Cambridge Analytica: The Story so Far, even seemingly trustworthy organizations can often do unethical things with user data. In this example, Cambridge Analytica was accused of using access to personal information to attempt to sway political election results.
Net Neutrality has been a hot topic since it was dissolved at a federal level in the United States in 2017. The article Net Neutrality Is Officially Gone. Here's How This Will Affect You written by Dan Robitzki details the potential fallout of this decision. Net Neutrality ensured that the internet remained a free and open resource. With these rules gone, internet service providers will be able to slow or block specific types of internet traffic and charge premiums for reasonable speeds and access. In discriminating between different user’s traffic based on the content they access or the type of content they can afford to access internet service providers will be breaking the ACM Code of Ethics section 1.4 Be Fair and Take Action Not to Discriminate.

Internet tech corporations have a tremendous amount of leverage and influence in the debate on net neutrality. One step that I could take as a browser developer is to take a clear stance on the issue like Mozilla did as detailed in their blog post Mozilla Fights On For Net Neutrality. Statements such as this effectively send a message about the importance of net neutrality. Another way is to simply not participate in the inevitable unethical actions that internet service will take. Refusing to pay unfair premiums to increase the speed of a website will be a statement in itself against such predatory tactics. While this approach is unlikely to make any fundamental changes, it is important nonetheless to act ethically and not participate in unethical business practices. A third and probably far fetched method for fighting for net neutrality that a browser developer could take is to disguise user traffic. This would mean taking efforts to make sure that information that internet service providers could use to restrict access are not included in the packets that are sent from the browser.
Copyright violations are a significant problem online. As detailed in the article *Internet Piracy: The Effects of Streaming Services and The Digital Marketplace* by Jake Nevola, internet piracy has resulted in the loss of significant profits in the entertainment and software business. Acting ethically in respect to online copyright means adhering to the ACM Code of Ethics section 1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

In addressing copyright issues in browser development, there is a fine line between attempting to restrict user access to media that violates copyright law and violating the privacy of the user. When the distinction between a legal and illegal activity cannot easily be made, such as whether a .torrent download contains copyrighted material or not, no action should be taken. Looking closely at the user data would be a violation of their privacy. Another way the problem of copyright violations can be addressed is to implement strong DRM policies. Web DRM is discussed in the article *What is Web DRM and How Does It Affect You?*. Web DRM technology allows content creators to allow users convenient access to content that they have a right to access while blocking access to those who do not. A strong web DRM engine in a browser can help stop people from using the browser to access illegal materials. A third method for addressing the problem of copyright violation is to warn users who attempt to access websites that often host copyrighted material. Uneducated internet users can access illegally uploaded media without knowing it. Warning them of this possibility before hand could effectively solve that problem. This method would also walk a fine line between ethical action and violating user privacy.
The problem of enforcing digital rights management and copyright laws while still respecting the privacy of users is an issue that could potentially require me to blow the whistle. While enforcing copyright law is important in protecting content creators, it should always be done in a way that does not violate the privacy of others. In response to unethical handling of user data, information could be reported to The Association of Computing Machinery if the responsible company is a member of the ACM. If not, the violation could also be reported in relation to the Electronic Communications Privacy Act.

The process for reporting a breach of the ACM Code of Ethics is detailed on their page [ACM Code of Ethics Enforcement Procedures](http://www.acm.org/about/ethics). Ethics violations are to be sent to either the head of the ethics committee or to the president of the ACM. If the ACM finds unlawful behavior in their review and consideration process, the appropriate authorities will be informed. The ACM will decide the appropriate action to take in order to fix the issues that brought about the ethics code breach and carry them out. If it is deemed necessary, other members of the ACM will be notified of the event and the actions taken as consequences. Protections for whistleblowers after the fact are also included in the code of ethics. Any retaliation against the whistleblower is strictly prohibited under these protections. Reporting violations of the Electronic Communications Privacy Act can be directed to the Justice Department. As discussed in [Electronic Privacy Rights: The Workplace](http://www.epri.org/privacy-workplace), accessing private information is illegal. If found to have potentially violated the Electronic Communications Privacy Act, organizations will be brought to a United States court to determine to what degree the law was violated and the appropriate course of action.
In making my decisions for the five dilemmas I used the rights approach to ethical decision making. The article *Five Ways To Shape Ethical Decisions: Rights Approach* discusses the technicalities of the rights approach. According to the article, the right to choose how we live our lives is paramount to most others. Therefore in situations such as the enforcement of copyright laws on the internet, the rights of the user to privately access legal information should be considered very important. This means that unless there is significant evidence that they are taking part in illegal activities their business should remain only their own.

Like the copyright infringement issue, the problem of identifying information being included in datasets that are mined by third parties should also be considered under the rights approach. People have a fundamental right privacy, and when their anonymity cannot be guaranteed, their participation in these programs should be for them to choose. This is why I offer opting out of these programs as a potential solution to the problem. Additionally instead of burying these terms in countless pages of legal jargon in the form of a EULA, users should be presented with the facts in clear and understandable terms. This puts control over how private their lives are directly into their hands.

The rights approach to ethical decision making can also be applied to the net neutrality issue. The principles behind the rights approach to ethical decision making state that people should have the right to engage in any contractual agreement that they wish to and be guaranteed whatever the contract states. Under current federal laws regarding net neutrality, cable companies are not required to be transparent about their services. This makes the right to receive service in accordance with the terms of the contract impossible.


Bibliography
