Ethical Imperatives in API Development: Safeguarding Privacy, Security, and User Trust in the Digital Ecosystem

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Morgan Campbell Kinne

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisors

Richard D. Jacques
Department of Engineering and Society

Peer Edit Notes

The process of writing this paper included receiving comments from my peers in STS 4600. I received help from Olivia Luu and Nikki Akula. Nikki Akula provided feedback on the grammar and sentence structure of the paper, helping proofread. Olivia Luu commented on grammar and sentence structure, as well as giving feedback on the content and suggesting more context and analysis in some sections, helping to round out the paper. I followed their suggestions to edit this research paper.

STS Research Paper

The world we live in today is heavily dependent on functional software. Application Programming Interfaces (APIs) are the backbone of software in the modern world; without the interconnectedness APIs provide, our society would not function as seamlessly as it does today. APIs facilitate quick and easy communication and integration between software systems. From enabling social media networks and e-commerce transactions to powering cloud-based services and Internet of Things (IoT) devices, APIs play a vital role in the transformation of technology across industries. IoT, for context, refers to the network of physical objects that are connected through networks. As things such as IoT devices are becoming commonplace in our daily lives, with many people being able to control home devices such as smart thermostats and smart lights from the convenience of their phone, it is important to recognize how much we rely on that convenience–and consider the new vulnerabilities we must factor in when designing the software systems that serve those devices.

In parallel with this technological advancement, there is a growing recognition of the need for engineers and organizations to prioritize ethical values in the development and maintenance cycle of products, including APIs. Those involved in both the development of APIs need to be conscious of the ethical responsibilities that come with them. Ethical considerations such as breaches of data privacy, security vulnerabilities, accessibility, diversity and inclusion, and fair-use principles are increasingly crucial in shaping the digital landscape. Without addressing the ethical issues related to these topics, the digital world will not be able to function sustainably or inclusively.

In this paper, I will argue that it is vitally important to address the ethical issues related to APIs in both design and maintenance, which should be considered in depth by the engineers and organizations that build these products. Users should be careful with the data they provide to these APIs. Ignoring the ethical principles of software and, specifically, API development will undermine user trust and damage the reputation of organizations, posing systemic risks to the integrity of the digital infrastructure. There are also considerations regarding legal use and fair-use principles, which could have large impacts on companies using and developing APIs. Ethics in API development should be prioritized with the goal of fostering a culture of responsible innovation, with the mindfulness to ensure that APIs serve the interests of a society. I've explored several ethical issues related to APIs, such as the effects of data privacy and protections, cybersecurity and vulnerabilities, and considerations regarding accessibility and legality. I examined papers on the impact of ethical practices in API development, and case studies of data leaks and their impacts on an organization's reputation and how protections can be built into software as Terms of Service (ToS), with the intent of protecting the users. I will also delve into the strategies and best practices for addressing ethical concerns within API development, offering recommendations for ethical decision-making and accountability.

Through relevant literature, I will examine different case studies of ethical dilemmas faced during the development and maintenance of APIs, providing insights into the real-world implications of neglecting ethical rules during development. Within this paper, I will attempt to encompass the importance of addressing all concerns related to ethics in API development, with the goal of safeguarding privacy, security, and user trust in the digital ecosystem, offering recommendations for ethical decision-making and accountability.

Sociotechnical Framework

The sociotechnical framework outlined in this paper underscores the intricate interplay between technological design, societal values, and ethical considerations in API development. Through concepts such as values and value-laden design, we recognize the inherent subjectivity in design decisions, emphasizing the need for conscious and ethical design practices that prioritize the well-being of all stakeholders. The concept of responsible research and innovation (RRI) further emphasizes the proactive role of engineers in anticipating and addressing social implications, fostering inclusivity, and adapting to evolving societal needs.

Moreover, ethical theories such as utilitarianism and deontology provide valuable lenses through which to evaluate the ethical dimensions of API development. While utilitarianism prioritizes the maximization of societal happiness and utility, putting an emphasis on what people experience because of a choice made in design, deontology emphasizes moral duties and principles, guiding engineers towards actions that align with ethical imperatives and responsibilities by navigating the importance of adhering to rules and obligations.

As we navigate the complex landscape of API development, it is imperative to recognize the ethical implications inherent in the design, deployment, and usage of APIs. By integrating ethical considerations into every stage of development, from initial design to ongoing maintenance, developers can mitigate risks, safeguard user privacy, and foster trust in the digital ecosystem. Moving forward, continued collaboration, transparency, and adherence to best practices will be essential in ensuring that APIs serve as engines of innovation while upholding ethical standards and societal values.

Value of Application Programming Interfaces and Conscious Design

APIs play a pivotal role in today's digital ecosystem, helping to foster innovation by allowing developers to build upon existing functionalities and integrate various services into their applications. In many cases APIs help with a quick transfer of data between systems, providing a seamless connection between these systems. This accelerates the development of new solutions, driving technological advancements across industries. For instance, APIs enable the integration of payment gateways, mapping services, social media platforms, and countless other functionalities into applications, further enhancing the user experience and expanding the possibilities for software development.

Moreover, APIs enable businesses to leverage the abilities of external developers and partners, effectively enabling them to achieve beyond what their internal resources are capable of. By providing access to their services and data through APIs, companies can reach an extensive network of innovators, contributing to a strong ecosystem of third-party applications and services. This improves the value of products and services and creates new opportunities for streams and business opportunities. Conscious design when developing APIs is crucial for maximizing the value and effectiveness of the software. A well-designed API is intuitive, flexible, easy to use, and was developed with ethical principles in mind. This empowers developers to quickly integrate it into their applications with minimal effort and cost. It is important to factor in these considerations to ensure that all APIs remain scalable, secure, and reliable, especially as usage patterns change over time (Wolf, 2020).

Conscious design gives API providers the ability to align their offerings with their strategic objectives and target audience, whether their goal is to maximize return on investment (ROI) for stakeholders, foster ecosystem growth, or drive innovation. By considering the needs and preferences of developers and users, API providers can tailor their API to deliver maximum value and achieve the desired goal. APIs play a critical role in driving innovation, enabling collaboration, and expanding the reach and capabilities of businesses and developers alike. Through conscious design and strategic planning, API providers can unlock the full potential of their capabilities, driving progress and creating value for their customers.

Importance of Data Privacy and Security in API Usage

APIs enable the exchange of data and interactions between different software applications, connecting them across platforms. However, with this interconnectedness comes dangers such as the risk of data breaches or misuse of user data. This means that the responsibility to prevent breaches and ensure APIs provide security, privacy, and accessibility to these users falls to API providers, which includes the developers and the organizations (Kocot, 2023). The term 'data privacy' refers to more than just protecting the data from malicious intent, it also involves maintaining a level of respect for the users and allowing them to control and know which sources their data is made available to. This involves sharing with the user the parties that have access to their data, how it's being used, and whether the organization with access is profiting from having this access.

Data security, on the other hand, refers not just to protecting user data, but also protecting the API itself. There are many security measures that are commonly implemented with the intent of protecting APIs and their data, including authentication, which involves verifying the user's or system's identity as the API request is made; authorization, which checks the permissions of the authenticated user before performing any actions; and encryption, which involves the process of encoding data so that only authorized parties can read it (Kocot, 2023). There are many other techniques that can be used to secure an API, such as ones that protect the API from abuse and other malicious activities.

When handling ethics related to API, we also need to discuss the ethics of accessibility and fair use principles. Accessibility in APIs refers not just to the actual use of the API, but also the services it provides. APIs exist with the goal of allowing people to use and benefit from the connectedness of the internet, and they should attempt to promote a culture of inclusivity. On the other hand, fair use principles are related to the legal and ethical boundaries of using an API. All APIs are written with a ToS which includes guidelines that users of the API need to follow. All ToS refer to protecting user data during usage and storage, so that the data supplied by the API will not be endangered while the API is in use (Kocot, 2023). Without considering these principles, API providers endanger their users and expose themselves to legal issues and loss of user trust.

Dependency on APIs and Vulnerability of User Data

As society rapidly becomes more dependent on technology, technology has to adapt to handle increased load and demands. In recent years, there has been a massive shift from using and implementing closed applications – also known as closed source or proprietary software, where the source code is not available to the public and therefore cannot be modified or seen – to giving preference to open-source software – where the source code is readily available and easily modified. This functions well with the massive growth in technology because it allows more users to contribute to a project with the goal of improving the software. However, this also exposes the software to exploitation and dangers that do not exist at the same level with closed source software. The increased use of open-source software comes with benefits such as the ability of users to contribute positively and identify any security issues to be fixed, however the drawbacks can put the users of the software in great danger.

An example of open-source software is the open information sharing available with Web APIs, which provide the data supplied to them readily to other sources, such as in an exchange of services between the API and the source supplied with said data (Ichario et al., 2020). This highlights the evolution of web technologies with the idea of improving the user experience by providing their data to any third-party source that requests it. As the adoption of Web APIs for open information sharing increases, this sets the stage for the importance of understanding issues related to ToS and privacy.

The vulnerability of user data can be highlighted by an example interaction between a user and an API. In this situation, I, the user, am interacting with a travel website, trying to book a hotel. I'm entering secure data into the travel website, such as my name, dates of travel, location, budget, and more. As I enter my information into this website, I have an unspoken agreement that the API used on this website will not expose my entered data to third parties unless it is necessary. This API is probably sending my information to a massive collection of relational databases to find the best price for my travel needs. While yes, this may benefit me in finding an affordable hotel, my information is now available to a wide variety of parties, some of which may be malicious, or at the very least unwanted. Companies such as Facebook have consistently sold user data and surveys show a massive decrease in user trust after this was exposed, specifically in relation to the user's privacy (Weisbaum, 2018). Users rely on web software to be secure to a certain extent, and it is the organization with access to this data that must be mindful of how they respect the user's privacy.

Case Studies on Addressing Ethical Issues in API Development

Sometimes the ethical issue faced might not have to do with the API developer but rather the developer using an API. Sometimes when a developer is implementing a project that uses an API, they might discover incompatible data and privacy policies, such as a situation where the purposes the developer needs the API for might violate the ToS of the API. In this case, the developer using the API needs to uphold the ToS and respect the requirements of the API. The reuse and replications of ToS among API providers can lead to misunderstandings regarding the compatibility of different APIs with developers' applications. This can result in situations where developers may abandon their efforts towards the API integration and start with a new API which aligns with the project requirements (Ichario et al., 2018). This situation not only disrupts the development process but also affects the time and resources already invested in the project. Moreover, the all-or-nothing approach of ToS provides very little flexibility for developers to customize the terms specific to their project. These challenges highlight the importance of considering ethical implications in API development, particularly in respecting the ToS of an API with regards to data privacy, to avoid potential consequences such as project termination and wasted efforts. Lessons learned from such cases emphasize the need for clearer communication and collaboration between API providers and developers to ensure ethical API usage and mitigate risks of data breaches and privacy violations.

Another important part of the ethics behind API usage refers to data anonymization. The implications and challenges that come with anonymizing data, in regard to protecting users whose data is made available for situations such as empirical research, are increasingly complicated by the sharing of data sets among researchers especially when publishing data and analysis (Lomborg et al.). In research situations where the information and depth of analysis could expose sensitive information about users, the value of the information and the handling must be careful not to discard the risk of violating the trust and expectations of the user providing the data. Researchers have noticed that social media companies which previously provided access to API's containing data relevant to empirical research have stopped providing free access and are instead switching their approach to prioritize monetization from the data provided (Lomborg et al.). This issue underscores a darker shift towards capitalization of data available from APIs, which further goes to show the risks that exist when a company would rather profit from data, which is rarely anonymized, versus trust a research team to anonymize and study the data.

Strategies and Best Practices for Ethical API Development

While prioritizing data privacy and security, ethical considerations should be integrated into every stage of API development, from the first stage of development to the continuous maintenance cycle. Looking at how current practices regarding Web APIs allow every site access to every feature within a browser, we can identify that a better alternative is to restrict websites to a subset of safer functionalities, focused on serving the user (Snyder, 2018). This approach prioritizes user security by granting functionalities to services based on their relevance and necessity to the goal at hand. This research underscores the importance of fostering a culture of responsible innovation and accountability in API development practices. By adhering to practices and frameworks such as privacy by design and security by design principles, developers can proactively find and account for ethical implications in API design. This involves conducting thorough risk assessments, implementing privacy-enhancing technologies, and offering transparency to users regarding data collection and usage practices.

One security practice that could be applied to web applications is ‘least-privilege’, which restricts the functionality of websites and the information they have access to just to those which are necessary for their current use (Snyder, 2018). Limiting the availability to user data to minimize the risk of unauthorized or unnecessary access is one application of data privacy and security. Findings indicate that implementing security techniques strongly improves privacy and security with only a small cost to the experience of the user (Snyder, 2018). Developers and organizations need to understand the benefits of increasing privacy and security and thus building up user trust with how the user’s experience may change on their website, and account for such in their product. They must be held responsible to implement measures to safeguard user data and mitigate the risk of data breaches. By adhering to best practices and industry standards, such as encryption, authentication, and access control mechanisms, developers can ensure the safety of user information within their APIs.

Conclusion

In conclusion, this paper has highlighted the importance of addressing ethical considerations in the development and maintenance of APIs. APIs will continue to support the massive system of the connected online world, facilitating seamless communication and integration between various systems and platforms. However, along with this level of interconnectedness comes the responsibility of developers and organizations to prioritize data privacy, security, and accessibility. The discussions in this paper have covered the multifaceted nature of ethical issues related to API development, ranging from data privacy violations to cybersecurity vulnerabilities and considerations regarding accessibility and fair use. Through case studies, literature reviews, and news articles, I have examined the real-world implications of neglecting ethical rules during development and maintenance, emphasizing the value of ethical decision-making and accountability throughout the software development lifecycle.

For future considerations, it is important for developers and organizations to foster a culture of responsible innovation and ethical API development practices. This involves taking ethical considerations into account at every stage of API development, from design to maintenance, and ensuring transparency between API developers, providers, and users. Furthermore, industry standards and best practices, such as privacy by design, security by design, and least-privilege, should be used to proactively handle ethical situations in API design and implementation. By following these practices and frameworks, developers can mitigate risks of data leaks, privacy violations, and security vulnerabilities to maintain user trust and ensure a safe, inclusive, and sustainable digital future.

It is dire that developers and organizations understand how prioritizing ethical values in API development is essential for protecting user privacy and security, and also for upholding the integrity of the digital world and growing user trust. There is a collective responsibility shared by all developers, organizations, and users of the internet to promote innovation while respecting fundamental privacy and security principles. Through collaboration and renewed commitments to ethical decision-making, we can build a more ethical and resilient digital landscape for generations to come.

References

Ichario, Aidah, and Maarek, Manuel. "Vision: Investigating web api developer experience in relation to terms of service and privacy policies." In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 166-171. IEEE, 2020. doi: 10.1109/EuroSPW51379.2020.00030.

Kocot, Daniel. 2023. "APIs and Ethics." Architectural Bytes. August 7, 2023. https://architectural-bytes.ghost.io/apis-and-ethics/#:~:text=%2D%20Data%20breaches%3A%20If%20an%20API,whom%20the%20data%20is%20shared.

Lomborg, Stine, and Anja Bechmann. "Using APIs for data collection on social media." The Information Society 30, no. 4 (2014): 256-265.

Snyder, Peter E. "Improving Web Privacy and Security with a Cost-benefit Analysis of the Web API". University of Illinois at Chicago, April 17, 2018. https://hdl.handle.net/10027/22660.

Weisbaum, Herb. "Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal", NBC News, April 18th, 2018. https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011.

Wulf, Jochen, and Ivo Blohm. "Fostering value creation with digital platforms: A unified theory of the application programming interface design." Journal of Management Information Systems 37, no. 1 (2020): 251-281.