How Responsiveness and Anticipation can Guide the Ethical Design of Location-based Services

A Research Paper in STS 4600

Presented to the Faculty of the School of Engineering and Applied Sciences
Unviersity of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Engineering

Author

Rohan Taneja
May 11, 2021

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

Signature __Rohan Taneja______________________________ Date __________

Approved ____ Date __________
Rider Foley, Department of Engineering

Introduction

Over the past several years, user privacy issues associated with internet and technology companies have been brought to light more than ever before. Major privacy concerns have stemmed from location-based services (LBS), with companies like Apple putting several restrictions in place recently to prevent popular social networks like Facebook and Whisper from discretely collecting location data. By using real-time geolocation data collected through smartphones, corporations are able to leverage user location data to provide personalized services from mobile workforce management to proximity-based marketing (Goodrich, 2020). Location data can be collected within several meters through sources such as Wifi triangulation, in which locations are pinpointed based off signal strengths of nearby WiFi networks, or Global Positioning Systems (GPS), satellite-based navigation systems that can approximate a user's position based off cellular signals (Ho et al., 2015). Corporations have also begun using Bluetooth beacons, cell triangulation, IP addresses, or combinations of these to track a user's movements with more precision and accuracy than ever before (Ho et al., 2015).

The development of such precise LBS technology has had profound positive effects on the utility of smartphones and internet devices in a variety of use cases. Mobile applications such as AT&T's *Friend Finder* and Apple's *Find My Friends* tracking applications have enabled their customers to disclose their location to close friends and family as a safety mechanism and social proxy (LaMarca & de Lara, 2008). Commercial truck drivers and bus fleets can convey real-time location data to delivery centers to coordinate shipping and track assets for many large retail corporations. The company Foursquare is well-known for pioneering the integration of LBS into smartphones by allowing users to discover new local businesses and giving business owners a way to create location-based advertisement campaigns. Furthermore, LBS technology has created significant value for smartphone users in other applications such as ride-sharing apps, health wearables, fraud prevention, and more.

Despite the pervasiveness and social utility of LBS technology in nearly every industry, privacy concerns about the handling and collection of location data have negatively influenced Americans' perception of these technologies. One 2019 survey on Americans' perception of data-driven services found that 81% of Americans surveyed found that the potential risks of data collection by American companies outweighed the potential benefits (Auxier, 2020). The legal domain of electronic privacy laws has remained a gray area, as the few existing privacy regulations such as required privacy policies have done little to enforce privacy protections. In the same 2019 survey, just 22% of Americans who read privacy policies claimed to have read the policies all the way through (Auxier, 2020). The lack of transparency and privacy implications of LBS pose a potential threat to future adoption of this technology, and developers must take anticipatory measures in the planning, design, development, and maintenance phases of these technologies to mitigate privacy violations and repercussions among their platforms' users. The goal of this research is to examine how ethical and social considerations can help improve the planning and implementation of LBS to make these platforms more trustworthy for all. This paper will use a framework of responsible innovation to explore how anticipatory techniques and responsive design can achieve the responsible development of privacy-preserving location-based platforms.

Enabling the Responsible Innovation of LBS Technologies

Responsible innovation is a theory that describes how the technical design process involves both innovators and societal actors who are mutually responsive to each other with regards to the "acceptability, sustainability, and societal desirability" of the product being developed (Schomberg, 2012, p. 47). In *Developing a framework for responsible innovation,* Stilgoe et al. (2013) defines anticipation as a major societal aspect of responsible innovation that calls on scientists and innovators to practice foresight of detrimental implications involving both primary and secondary stakeholders of their products. Anticipation forces technology developers to consider different contingencies early in design process to increase resilience and guide "socially-robust risk research" (Stilgoe et al., 2013, p.1570). Developers can practice anticipating risks with systematic techniques like horizon scanning. Horizon scanning is a technique for informing decision makers about future threats for a product by methodically considering what technologies and social trends can be considered constant now and what might change in the future. When developing location-based platforms, anticipating potential implications with this form of scenario-planning can help guide the design process to prevent improper use of location-data and increase trust among the platform's stakeholders.

A survey of stakeholder engagement can offer valuable insight into what unintended scenarios are possible surrounding LBS technology, particularly relating to user privacy. In a detailed review of location-based technology, Abbas, Michael, and Michael argue that the two prominent ethical dilemmas associated with location-based platforms are "the risk of privacy breaches" and "the possibility of increased monitoring leading to unwarranted surveillance by institutions and individuals" (2014, p.11). To anticipate the severity of potential privacy breaches, LBS creators should be cognizant of how privacy breaches might affect key stakeholders when organizing their data. Stakeholders such as investors and sponsors of location-based technology might experience financial consequences resulting from less users on the app and a damaged reputation. Unwarranted surveillance and improper handling of location-data could entail additional stakeholders such as policymakers and government research agencies who may take regulatory actions to protect the privacy of users. For example, the European Union implemented the General Data Protection Regulation (GDPR) in 2018 to enforce strict standards on the tracking and collecting of identifiable data, including location-data (Huang et al., 2018).

Scenario planning requires leadership to consider from a long-term perspective the weaknesses and threats that can result from an insufficient understanding of how LBS customers will shape the use cases of a product (Schoemaker & Mavaddat, 2000). For location-based technology, developers might consider anonymization and cryptography methods that could minimize data breaches as the platform scales to more customers. Scenario-planning may even entail predicting what financial and competitive incentives a company's affiliate partners may have later on for collecting customer location data to establish and screen strategic partnerships. Furthermore, a stakeholder analysis can help guide identify the most prominent user groups to determine how the social outcomes of LBS may be molded by the way users interact with the product. By anticipating the privacy concerns of key stakeholders for a location-based platform, scientists and innovators can account for potential societal resistance with predictive measures taken early in the design process.

Beyond the planning and development of LBS technology, creators of LBS should consider how an interactive product and changing consumer market might inform how a stakeholder engages with a technology product. Responsible innovation coins this as 'responsiveness', or "adjusting courses of action while recognising the insufficiency of knowledge and control" (Stilgoe et al. 2013). According to Stilgoe et al., one significant criticism of LBS that has affected public engagement is the limited capacity for empowering social agency in technological choice. Through responsive design, creators can adjust for this insufficiency of knowledge on how users will react to LBS by creating more interactive and modularized interfaces. Responsiveness is another dimension that can contribute to the responsible design of location-based technology, in which indicative techniques such as value-sensitive design can guide the integration of human principles and ethics into the engineering process. By nature, a responsive design can encourage more interaction and control and empower users with more agency in controlling how the product can be used. Responsiveness thus aims to increase transparency and user-centric design, which is vital to improving this invasive perception and assuring future adoption of mobile LBS.

Case Context

Applications for LBS have evolved to work in indoor environments, such as for location-based advertising in shopping malls or museum virtual tour guides. However, in a research study on the evolution of location-based services, Huang et al. (2018) suggested that location-accuracy for mobile platforms like Waze and Parkbob is still often compromised in dense urban environments. To overcome these challenges, several advancements have been made by smartphone makers and LBS companies to provide more accuracy in positioning smartphones than ever before. According to *Nic Newman's Apple iBeacon technology briefing* (2014), mobile iOS devices with iOS versions 7 and later can now enable accurate location-sensing in close proximities through the integration of the "Core Location" application programing interface (API). Apple's Core Location API provides programmable software that synchronizes with

Apple iBeacons, which are small, embedded Bluetooth radios in iOS devices that can emit short-range signals (Newman, 2014). Fingerprinting localization is another technique used to position locations in complex indoor environments by approximating the radio signal strength (RSS) of a smartphone from fixed WiFi access points. A combination of BLE beacons and this fingerprinting technique has also been shown to further increase localization accuracy by verifying RSS measurements with relative distances from Bluetooth devices (Kriz, Maly, & Kozel, 2016). Although these technology advancements have provided real utility in many applications, they have also required increased surveillance through indoor location-positioning. To mitigate the ethical issues that stem from advanced LBS, privacy-preserving algorithms and responsive design techniques should be used to improve public confidence in this technology and give more control to the user.

Anticipation in the framework of responsible innovation requires acknowledging areas of uncertainty about the risks and benefits of a product, especially in the realm of user privacy. In 2017, a data breach of a McDonald's delivery app in India led to the disclosure of personally identifiable information (PII) including home addresses and contact information belonging to millions of McDonald's customers (Kirk, 2017). The leak of this user data was caused by the aggregation of location data for tracking deliveries and personal information, damaging customers' trust in the delivery system and leading to several lawsuits. By considering how a LBS platform could infringe on user's privacy and deter new users, LBS can employ a variety of privacy-preserving techniques to provide value while collecting minimal data or de-identifying personal information. Many location-based platforms have begun using techniques such as anonymization with spatial generalization, where the relative distances between app users can be tracked but the exact location details of users are hidden (Duckham et al., 2007). The COVID-19 pandemic has accelerated this advancement in privacy-preserving technology with the advent of digital contact tracing, in which smartphone apps log anonymous interactions between users to identify points of exposure to the infectious virus. The Decentralized Privacy-Preserving Proximity Tracing (DP3T) protocol is a well-known implementation of how contact tracing can achieve the same purpose as any LBS platform using a decentralized and anonymous tracing system. The DP3T protocol works by exchanging temporary ephemeral ID (EID) codes when users are in close contact, or within range of the Bluetooth beacons on their smartphones, to log a potential exposure (Schmidtke, 2020). These codes are stored locally on each user's device, and a positive COVID test will allow a user to broadcast the unique EID codes of their recent contacts to the secure DP3T web server (Schmidtke, 2020). The code will then be compared with the recent EID codes stored locally on the DP3T app to notify a user of a recent exposure (Schmidtke, 2020). By performing the bulk of computation locally and using randomized EID codes instead of personal information, the protocol can act on proximity information without identifying users or storing geographic data (Schmidtke, 2020). By anticipating concerns about government surveillance, the Switzerland government was able to use this protocol in its SwissCovid app to provide a non-invasive and opt-in contact tracing system for its citizens (Leprince-Ringuet, 2020).

Aside from anonymization and cryptographic techniques, developers of LBS must consider how 'responsiveness', yet another crucial principle of responsible innovation, of the app's user experience can create more transparency and trust by educating users on how their information will be used. One research study examined the impact of location-based social networking on trust between college students by gathering quantitative data through five focus groups of around 15 students enrolled in professional ethics courses (Fusco et al., 2011). Each focus group was asked a series of qualitative questions on the social implications of location-based technology and how it affected relationships with groups of people including family, friends, co-workers, government entities, and commercial entities. The results of this study highlighted privacy as one of the most frequent concerns of college students using these mobile platforms, particularly among those who did not fully understand what data they were sharing to their location-based network. Privacy can be incorporated into design by allowing users of location-based services to choose between different privacy modes, which alleviates uncertainty by giving users the freedom to understand and control all of the information they share. In 2019, Facebook enabled users to disable background location settings on the Facebook app and choose when the app is allowed to collect location data while open (Gesenhues, 2019). Although this may hurt prospects for partnered businesses looking to send advertisements to nearby Facebook users, it highlights a growing trend in location-tracking platforms to give users more control of sensitive data. Apple recently rolled out the Ad Tracking Transparency (ATT) platform with iOS 14, requiring all app makers to obtain consent from the user, as opposed to a simple opt-out feature, to collect or transmit location and other personal data or risk being banned from the App Store.

Research Question and Methods

The guiding question for this research will be: How can anticipation and responsiveness guide the responsible design of LBS platforms to mitigate infringements of user privacy and customer trust? This research focus will require further analysis into how anticipation can guide the long-term vision for a LBS and how responsiveness can cultivate its responsible design. By understanding how anticipation and responsive design can shape the social outcomes of sociotechnical systems, this research will inform how creators of this technology can incorporate ethical design principles in the planning of LBS platforms.

The first approach that will be used to pursue this research question will be analyzing case studies of location-based platforms that were both successful and unsuccessful. Case studies will be a useful research method for this research question because they provide concrete historical evidence of how the technical design of location-based platforms can lead to unanticipated consequences that can be improved upon with this technical project. The first two case studies examine how the design and planning of LBS led to negative social outcomes through a design that provoked uncivil user behavior and poor anticipatory measures that led to significant privacy violations. The next two cases explore how incorporating ethical considerations early into the design process can guide the implementation of a privacy-focused LBS. The second approach will be conducting a content analysis through an interview with an entrepreneur in the field of LBS. The purpose of interviewing entrepreneurs will be to gather deep insights on the current state-of-the-art in location-based technology and how privacy preservation techniques are being used in both the public and private sectors. This analysis will provide insight into the current landscape for implementing privacy preservation in LBS and provide expert opinions on how responsiveness can play a role in encouraging transparency across the LBS industry.

Results

The agency that users have in interacting with LBS platforms has a significant influence on the social contexts in which the LBS is used, and thus ethical LBS design must be focused as much on the behavioral patterns of users as the technical features of the system. To achieve responsible design, successful LBS platforms should use a combination of anonymization techniques, user-controlled design, and transparent policies early in the design process to create more ethically robust LBS technologies. For example, location data can be collected without being linked to identifiable user information to satisfy most use cases that depend on tracking aggregated location data. Additionally, LBS platforms should provide opt-in user agreement forms to collect location data, as well as interface controls over where and when data is collected to garner more trust from disparate user groups.

To understand how anticipation and responsiveness can affect the social outcomes of a LBS, I reviewed four case studies of LBS platforms with varying social outcomes and examined the moral dimensions of these technologies. Through these case studies, I gained a deeper understanding of how tenets of responsible innovation can be integrated into the planning and design of LBS to create more ethically robust platforms. I used these findings to dive deeper into how corporations are achieving responsible design today when handling sensitive location data, and I interviewed the CEO of a well-known LBS company to survey the future landscape for transparent LBS technologies.

Case #1: How the Sociotechnical Design of Yik-Yak Fostered Hate Speech.

In a case study on the location-based social networking app *Yik Yak*, Qinglan Li and Ioana Literat (2017) offer an in-depth analysis on how the hyperlocality features and user design of this app created a space for cyberbullying and hate speech. Yik Yak was created in 2013 as a social media networking platform that allows users to anonymously post unfiltered messages, or “yaks”, to a public message board shared by users within a 1.5 to 10 mile radius. Although the creators intended for this design to democratize the way users engage with social media networks, the platform soon became the source of great controversy at many college campuses across the United States. Many college Yik Yak boards became filled with racist and misogynistic comments with no mechanism to enforce accountability due to the app’s anonymous design. In late 2014, a series of student demonstrations took place at Colgate University in response to the racist messages against minority groups that had circulated to the top of the local Yik Yak board. Anonymous users in the campus Yik Yak board began posting targeted messages of violence towards the student demonstrators, and local police were unable to trace the users posting these messages due to Yik Yak’s policy for protecting the identities of its users.

In their analysis of the socio-ethical dimensions of Yik Yak’s technical features, Li and Literat demonstrate how responsiveness in social technology design can shape user behavior and create unintended consequences. By shielding the information of users and requiring only a user ‘handle’, Yik Yak’s anonymity protection leads to psychological effects that have been shown to provoke uncivil behavior in online settings. The anonymity allows for an online disinhibition effect, in which individuals are encouraged to ‘one-up’ other users with polarizing comments for more social engagement, and a bystander effect, in which users are less likely to defend victims of cyber bullying due to a complete lack of accountability. The app’s hyper-locality feature, or location-based communication, further amplifies voices of cyberbullying by allowing targeted messages to be posted anonymously to a community of friends, classmates, or neighbors. In other words, this hyper-locality combined with the app’s anonymity makes it especially easy for perpetrators to target victims they personally know.

Yik Yak offers a unique example of how seemingly neutral technology can affect power dynamics through its technical design and the agency it offers its users in amplifying voices of polarization. When analyzing the ethical implications of this technology, the responsiveness of Yik Yak’s design sheds light on how the interaction between the target users and the technology can cultivate unintended user behaviors. By considering how technical features can facilitate behaviors like the bystander effect, the creators of this platform might have been motivated to provide more moderation in Yik Yak boards. Furthermore, Yik Yak’s social and cultural context in college campuses could have informed better anticipatory measures to guide the ethical design of this platform early in the ideation phase.

Case #2: Care19 Contact Tracing Location Data Leaked by Third-Party

In 2020, the state government of North Dakota released a contact-tracing app to curb the spread of Covid-19 but failed to obtain a critical mass of users after news released that the app broke its own privacy policy. The app, Care-19, used geolocation features to anonymously cache the locations of its users several times per day to trace potential areas of exposure by infected individuals. Developed by a contracted technology company ProudCrowd, Care-19 was built to protect user privacy by assigning users with a pseudonymous numerical identifier when storing location data (Hamilton, 2020). The privacy policy for Care-19 outlined that this data would not be shared with any third parties, but months after its release, it was found that customer identifiers and location data were being sent to the location advertising company Foursquare.

In addition to location data, the Care-19 app was sending Foursquare the associated Advertising Identifier (IDFA) to uniquely link phones to users' spatial movements and track their behaviors for third-party location advertising (Hamilton, 2020). The aftermath of this news that companies were profiting off a public health crisis led to increased mistrust in the Care-19 platform. With less users on the app, contact tracing platforms are less effective at tracing infected individuals, and this likely affected public perception of other contact tracing platforms as well. The Care-19 platform provides an example of how unintended consequences can result from the mishandling of location data, and anticipatory measures like horizon scanning might have helped the North Dakota government in choosing a more trustworthy contractor. Furthermore, this highlights the difficulties of holding corporations accountable for violating privacy policies, and creators of platforms must consider the incentives of various stakeholders when anticipating the social impact of an LBS technology.

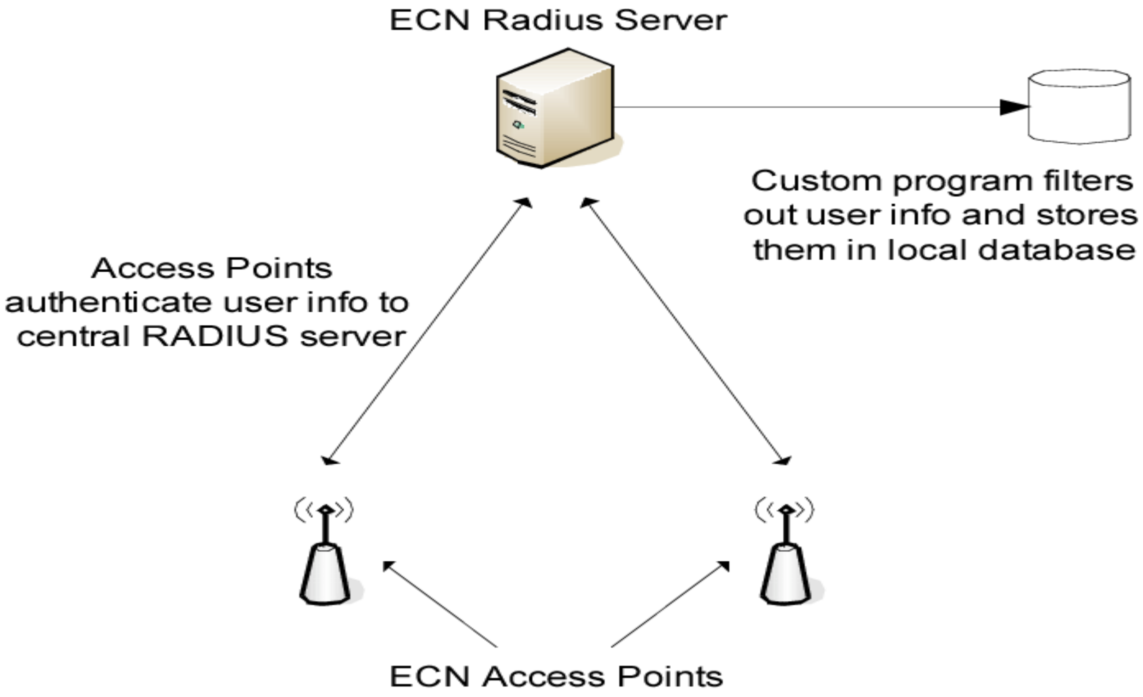
Case #3: Privacy-focused Location Discovery Service (LODS) at Purdue university

In a research study by Hoi-Ho Chan and Simon G. M. Koo (2007) on the ethical design of location-based wireless systems, students at Purdue University were asked to design an LBS under ethical constraints to determine how awareness of moral implications can achieve responsible design of LBS technology. Undergraduate students were tasked with building a transparent Location Discovery Service (LODS) to track mobility patterns based on student usage of the Purdue wireless network. During the project, mentors did not actively guide the design or implementation of the systems. The students were given a list of objectives to achieve ethical design: the prototype could not pinpoint particular users, the mobility record must be detached from user identities, and particular users should have the option to opt-in to track themselves.

The students positively responded to the ethical constraints introduced and even suggested further ethical concerns with their designs, despite the fact that the majority of students had taken at most two programming classes. They were able to successfully come up with a prototype using a local database and a series of access points on the Engineering Computer Network (ECN) Wi-Fi, as seen in Figure 1, which did not require the exact locations of users unless permitted (Chan & Koo 2007, p. 17).

Figure 1

Diagram of Student Prototype for Anonymized LODS


ECN Radius Server
Custom program filters out user info and stores them in local database
Access Points authenticate user info to central RADIUS server
ECN Access Points

The platform used an MD5 hashing algorithm to encrypt the MAC addresses of computer devices discovered on the network. The results of this experiment showed that awareness of moral dimensions in technology design could guide the implementation of ethical design considerations despite limited technical competencies. By anticipating ethical concerns early in the design process, the students were able to achieve all of the given objectives and build a LODS with several user privacy features. Furthermore, the students demonstrated that little technical competency was needed to create a responsive design by including opt-in features for users to decrypt their MAC addresses and track their mobility patterns if they chose.

Case Study #4: User-centered Design of a LBS App for Victims of Domestic Violence

Another case study by Walls et al. (2016) examined the impact of geolocation services on domestic violence survivors. For example, GPS technology is easily accessible through internet enabled devices and devices such as GPS ankle bracelets can be used to enforce restraining orders and track convicted abusers to protect domestic violence survivors. However, social media location networks and other GPS-enabled internet applications have also allowed criminals to locate survivors and monitor or harm them. The case study argues that digital literacy education and responsive design can help empower domestic violence survivors to protect themselves from location-enabled abuse and exercise control over their digital privacy.

In response to this lack of digital literacy, a research team created a location-based app, Safely Social, to allow domestic violence survivors to exercise more control over their geolocation information. The app has several responsive features to turn off all geolocation services on a mobile device, scan apps to determine where geolocation data is being collected, and silently notify a National Domestic Violence Hotline. Furthermore, the app anticipates several scenarios for domestic abuse by cloaking conversations and internet activity to hide the app's purpose when a survivor no longer has their phone. Although a survey of users suggested that the app was seen as useful, the study suggests that further research is needed to understand how technology design can improve technical literacy and empower more domestic violence survivors with control over their location data.

Interview with Joshua Anton, CEO of X-Mode

X-Mode is a growing startup that specializes in providing real-time location data from over 50 million monthly smartphone users to partnered app publishers through its proprietary software. I had the opportunity to interview X-Mode's CEO, Joshua Anton, to understand how one of the leading LBS players adheres to high ethical standards through privacy-focused design and strict data licensing policies. When I asked Josh what the leading factor that contributed to X-Mode's success was, he told me that X-Mode's commitment to providing transparency on both the publisher and consumer sides was vital to enabling the company to collect data in a trustworthy manner. One of X-Mode's key differentiators in its approach to privacy is opt-in informed consent, in which X-Mode's license requires publishers to provide app users with a consent screen to use X-Mode's location features. As Josh explained, most competitors still use opt-out legitimate interest, which is a more flexible GDPR regulation that allows publishers to keep data collection information hidden in the privacy policy and avoid asking users for full upfront consent. Josh mentioned that he tries to work as close to X-Mode publishers as possible and that his legal team conducts several monthly audits to enforce X-Mode's informed consent framework so that publishers collect data transparently. Furthermore, all users must be able to opt back out of location data collection and delete their historical records of location data if they choose. X-Mode Publishers risk having their software removed if an app is found in violation of X-Mode standards, and Josh believes that this no-tolerance approach will be necessary for the perception of LBS data collection to change. When asked about the future of X-Mode and the LBS industry, Josh put it this way: “I don’t regret being transparent in what we do, because I think that’s the way the location industry is moving. We just may have been a little too early for that to be fully accepted yet.”

Discussion

The landscape for LBS technology has evolved with more sophisticated data collection methods and increasing public scrutiny over user privacy concerns. This research demonstrates how a framework of responsible innovation can guide the responsible design of these technologies by anticipating the social behaviors of key stakeholders and incorporating this into a responsive design that gives users more control of their data. The Yik-Yak case provides a well-known example of how the social contexts of a platform’s users can shape the outcomes of the technology, and the Care-19 data leak is a recent example of how other stakeholders can influence the consequences of location data collection. The LODS service built by students from Purdue University suggests that little technical expertise is needed to build anticipatory features, and the Safely Social app includes various examples of responsive features that can give users more control over their data collection. Furthermore, Joshua Anton revealed the important role that opt-in forms play in building transparent LBS interfaces, and the strict enforcement of data policies allows X-Mode Social to mitigate the unintended social effects of their products.

When considering how technical and social design can shape the outcomes of LBS technologies, the Actor-Network Theory (ANT) approach can provide further insight by evaluating how various stakeholders will influence these technologies. ANT is a theoretical approach to understanding the relationships between technology and various stakeholders involved in related social processes. The Yik-Yak case presents a relevant example of how various actors in the app's network of college campuses could exploit anonymization features in the app to spread hate messages, which in turn led to social effects on other actors such as the bystander effects that further provoked uncivil behavior. In contrast, an app for domestic violence survivors was able to avoid these outcomes by anticipating how actors in the network of domestic violence victims and abusers may interact. These considerations were used to determine which responsive features would be implemented to allow victim of domestic violence to adapt to changing circumstances.

Although the case studies of the Purdue LODS study and the domestic violence app demonstrate how responsive features and anticipatory planning can create responsible design, these studies are limited by their metrics of success in mitigating unintended outcomes. Neither of these platforms have a critical mass of users on the scale of larger social media networks such as the Yik-Yak platform. Thus, it cannot be ascertained that the measures taken in designing them would have been completely effective in preventing unintended social effects that would result from a larger network of bad actors. Furthermore, the interview was conducted with only one major entrepreneur in the LBS field, and thus it is difficult to determine how commonplace X-Mode's privacy measures are in the LBS industry today.

To expand on this research, I would try to get in touch with entrepreneurs from smaller startups in the LBS industry, who may have been more receptive to sharing their company practices on user privacy. Furthermore, I would survey several frequent smartphone users to gather a data-driven consensus on how public perception is affected by responsive features for controlling user location data. I am curious to understand whether a majority of smartphone users value these features to have full control of their data collection, or if these features are predominantly viewed as annoyances and hence could be why many LBS companies are motivated to collect data more discretely.

As a technology enthusiast hoping to pursue a career in consumer technology, this research will be vital towards understanding how my products will fit into larger sociotechnical systems and how I can use anticipation and responsiveness to design ethical technologies. The success of consumer-facing technologies is dependent on public trust in using these products, and this research demonstrates how anticipating the misuse of technical features or flawed strategic partnerships may impact the outcomes of my products. Through horizon scanning of user behaviors, a privacy-preserving technical architecture, and a responsive user interface, this research presents various techniques I can use to achieve responsible design in consumer technology products.

Conclusion

By evaluating the design considerations and social outcomes of major LBS platforms today, this research demonstrates how responsible innovation tenets can be practically implemented to control the impact that LBS technologies have on their stakeholders. User privacy concerns have grown significantly with the increasing sophistication of location data collection, and creators of these technologies must consider how the technical and psychological aspects of design can exacerbate ethical issues resulting from their products.

Through case studies and live interviews, this research presents various approaches in which LBS platforms have attempted to achieve responsible design. By including responsive user features such as location collection controls and informed consent screens, LBS platforms can be more transparent in educating users on how their location is tracked. However, the technical design of these features must be weighed against the agency of users with malintent to change the power dynamics of LBS platforms and affect severe unintended consequences. For example, project managers should consider which stakeholders are affected by an LBS product in order to determine how interactions between these groups could cause negative social repercussions to arise, such as with the Yik-Yak stakeholders in college campuses. Additionally, developers should de-label location data to the furthest extent that still satisfies the LBS platform's use case, as this can limit the identification of users if a data breach is caused in the future by malicious actors. Thus, anticipation of user behavior and the relationships between technical design and potential stakeholders is critical in the early phases of LBS development to mitigate these outcomes. Furthermore, responsive design can provide enhanced transparency by granting more control to users in censoring their data and educating them on how their data will be used. Opt-in forms can force users to review how their data will be used, and modularized controls such as the ability to switch off location-tracking and toggle background-app usage can create more transparent LBS technologies. The core of LBS functionalities is the collection of user location data, and a lack of public trust can pose a threat to democratizing useful applications of LBS if this data cannot be collected in an ethical manner. As the industry of LBS moves towards increased transparency and regulation, developers of these platforms should utilize this framework of responsible innovation to sustain future adoption of this technology for years to come.

References

Abbas, R., K. Michael, and M. G. Michael. (2014). The Regulatory Considerations and Ethical Dilemmas of Location-Based Services (LBS): A Literature Review. *Information Technology & People 27*(1), 2–20. doi:10.1108/ITP-12-2012-0156.

Auxier, B. (2020, August 27). How Americans see digital privacy ISSUES amid the COVID-19 outbreak. Retrieved February 24, 2021, from https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

Chan, H., & Koo, S. G. (2007). Ethical and legal awareness in location-based wireless system design projects. *2007 37th Annual Frontiers in Education Conference - Global Engineering: Knowledge without Borders, Opportunities without Passports,* S2C-16-S2C-19. doi:10.1109/fie.2007.4418171

Duckham, M., M. Mokbel, and S. Nittel. 2007. Special Issue on Privacy Aware and Location-Based Mobile Services. *Journal of Location Based Services 1*(3), 161–164. doi:10.1080/17489720802089489.

Fusco, S. J., Michael, K., Aloudat, A. & Abbas, R. (2011). Monitoring people using location-based social networking and its negative impact on trust: An Exploratory Contextual Analysis of Five Types of "friend" Relationships. *International Symposium on Technology and Society, Proceedings*. doi: 10.1109/ISTAS.2011.7160597

Gesenhues, A. (2019, September 10). Facebook changes how it handles user location data settings in response to Android, iOS updates. Retrieved February 23, 2021, from https://martechtoday.com/facebook-changes-how-it-handles-user-location-data-settings-in-response-to-android-ios-updates-235395

Goodrich, R. (2020, October 14). Location-Based services: Examples and uses. Retrieved February 23, 2021, from https://www.businessnewsdaily.com/5386-location-based-services.html#:~:text=Location%2Dbased%20services%20use%20real,provide%20information%2C%20entertainment%20or%20security.&text=Location%2Dbased%20services%20use%20a,opted%20in%20to%20allow%20it

Hamilton, I. (2020, May 22). Researchers found North Dakota's CONTACT-TRACING app covertly sending location and advertising data to third parties. Retrieved March 27, 2021, from https://www.businessinsider.com/north-dakota-contact-tracing-app-violating-privacy-policy-2020-5

Ho, M., Lieberman, M., Gupta, V., Brautigam, K., Meckley, J., Davis, M., . . . Katyal, P. (2015, October). *Demystifying Location Data Accuracy* [PDF]. New York City: Mobile Marketing Association.

Huang, H., Gartner, G., Krisp, J. M., Raubal, M., & Weghe, N. V. D. (2018). Location based services: ongoing evolution and research agenda. *Journal of Location Based Services*, *12*(2), 63–93. doi: 10.1080/17489725.2018.1508763

Kirk, J. (2017, March 20). McShame: McDonald's API leaks data for 2.2 million users. Retrieved February 24, 2021, from https://www.bankinfosecurity.com/blogs/mcshame-mcdonalds-api-leaks-data-on-22-million-p-2426

Kriz, P., Maly, F., & Kozel, T. (2016). Improving indoor localization using bluetooth low energy beacons. *Mobile Information Systems, 2016*, 1-11. doi:10.1155/2016/2083094

LaMarca, A., & De Lara, E. (2008). Location systems: An introduction to the technology BEHIND location awareness. *Synthesis Lectures on Mobile and Pervasive Computing, 3*(1), 1-122. doi:10.2200/s00115ed1v01y200804mpc004

Leprince-Ringuet, D. (2020, May 28). The world's First CONTACT-TRACING app using Google and Apple's API goes live. Retrieved February 23, 2021, from https://www.zdnet.com/article/the-worlds-first-contact-tracing-app-using-google-and-apples-api-goes-live/

Li, Q., & Literat, I. (2017). Misuse or misdesign? Yik Yak on college campuses and the moral dimensions of technology design. *First Monday*, *22*(7). doi: 10.5210/fm.v22i7.6947

Newman, N. (2014). Apple iBeacon technology briefing. *Journal of Direct, Data and Digital Marketing Practice*, *15*(3), 222–225. doi: 10.1057/dddmp.2014.7

Schmidtke, H. R. (2020). Location-aware systems or location-based services: A survey with applications to covid-19 contact tracking. *Journal of Reliable Intelligent Environments, 6*(4), 191-214. doi:10.1007/s40860-020-00111-4

Schoemaker, Paul & Mavaddat, M.V.. (2000). Scenario planning for disruptive technologies. Wharton on Managing Emerging Technologies. 206-241.

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for Responsible Innovation. *Research Policy*, *42*(9), 1568–50. doi: 10.1016/j.respol.2013.05.008

von Schomberg R. (2012) Prospects for technology assessment in a framework of responsible research and innovation. *Technikfolgen abschätzen lehren* (pp. 39-61). doi: 10.1007/978-3-531-93468-6_2

Walls, D., Dieterle, B., & Miller, J. R. (2016). Safely social: User-centered design and difference feminism. In Blair, K., & Nicholson, L. (Eds.), *Composing feminist interventions: Activism, engagement, and praxis.* Manuscript in preparation.