A Case Study on Mobile Device Usage and Public Well-Being

Sai Krishna Reddy M

Nagarjuna Konanki

Nikitha Reddy Singu

Regis University

MSDS 640

Prof. Ghulam Mujtaba Ph.D.

May 4, 2024

Abstract

This case study explores the relationship between mobile app usage, personality traits, and perceived data control among users. With the growing concerns over digital privacy, many individuals report feeling disconnected from how their personal data is handled. Using a combination of personality assessments and app usage patterns, we investigated the "control gap" the mismatch between a user's consent and their belief in data ownership. Our analysis revealed significant disparities across age groups and personality dimensions, especially among users with high app engagement and low perceived control. We employed machine learning techniques, including Random Forest, to predict users likely to feel out of control, and also identify groups with similar behavior and psychological traits. These insights can support app developers in designing clearer consent mechanisms and more personalized digital experiences that align with individual user profiles. Ultimately, the goal is to bridge the gap between user expectations and actual data practices, promoting ethical and user centered digital environments.

A Case Study on Mobile Device Usage and Public Well-Being

Introduction

Cell phones are a part of our lives today, revolutionizing the way people communicate, work, watch entertainment, and even dress. Convenience in the form of online services has never been greater since the smartphone's arrival and ubiquitous apps. But with a cost the users themselves are not typically aware of how much of their own individual data they're releasing and how much of such data is being collected, monitored, and sold. Although consumers consent to download and use programs at no cost, a vast gap between digital surveillance and third party data exchanging reality and expectation of privacy is present.

It is public welfare matter in the internet community, and being in control of information is one to highlight. Perceived control is what the user perceives as in how it appears that the user has some rational conception and control over her or his information. In order to measure this, we define a new metric, the "Control Gap," which measures the gap between what users perceive they are agreeing to in terms of rights on data and what they actually agree to. The gap may bring about the experience of powerlessness, bafflement, and even anguish, especially among the most vulnerable segments, such as youth users whose lives are most predominantly lived through mobile contexts.

Our studies cut below use of app surface to investigate psychological, demographic, and behavioral predictors' influence on wellbeing among digital mobile users. Our data include variables for age, gender, app use categories, and personality traits that allow us to look at correlations between user categories and perceived control. In doing so, we construct towards practical conclusions that can inform ethical app development, simplified consent models, and improved mechanisms for user education.

By making patterns of mobile phone use available in data science, not only can we determine technical issues, such as where consent models fail, but psychological and social dimensions of digital technology adoption as well. In the globalizing world where virtual interactions more and more seep into "real" reality, safeguarding users from harm, informing

them well, and being nice to them in virtual spaces is a public good. This work is thus both a technical inquiry and an argument for digitally user friendlier worlds.Malgieri & Custers (2018)

Existing Solutions

In recent years, several strategies have been used to address issues related to digital well being, user privacy, and control in mobile app environments:

- **Privacy Policies and Consent Forms:** Websites and applications are meant to publish privacy policies and obtain consent from users prior to data collection. But the policies are always complex and fall below the radar of an average user, providing an illusion of control.
- **App Permissions Management:** Mobile operating systems (Android, iOS) provide full control of application permissions (location, camera, microphone, etc.) at the manual level. Still, the users are never inconvenienced or feel the effect in most situations.
- **Screen Time and Digital Well-being Tools:** The most recent operating systems and some programs even include usage dashboards (Android Digital Wellbeing, iPhone Screen Time). These programs are made to notify the user to more extensive device misuse but are lacking in providing any useful feedback.Berr (2019)
- **Simplified Consent Flows:** A few more recent platforms have also introduced robust, "layered" forms of consent that give users more control over the data points they'd rather provide. Velocity of user acquisition is valued by most apps more than informed consent.
- **Regulatory Efforts (GDPR, CCPA, etc.):** There are state laws requiring apps to safeguard users' personal data and request permission. The law strengthens the data

rights but there is partial enforcement and unawareness on the part of the majority of the users.GDPR (2018); Lisowski (2023)

Linden et al. (2018)Degeling et al. (2018)

Proposed Solution

This case study suggests the use of machine learning models, namely Random Forest classifiers, to predict users who will experience a lack of control over personal data. The model predicts users based on app behavior, age, education level, and psychological personality. The model predicts users with high "Control Gap" and users' difference between sense of ownership of data and actual control or degree of consent. Predicting these types of users enables designers and developers of apps to take steps ahead of time to fight user confusion or helplessness. The solution enables platforms to personalize intervention according to the individual risk per user.

For instance, users who are likely to be less data controlling can be shown more legible, simpler consent requests, contextual privacy alerts, or visual cues regarding what data is collected and why. An effort towards designing specific solutions for specific vulnerable user groups would not only contribute to user trust and digital competency but also adapt to ethical design of technology through being responsive to specific vulnerable user groups' exact needs. Digital platforms can enable transparency, fairness, and public welfare responsiveness via the integration of predictive intelligence within user facing systems. **?**Rizk et al. (2021)Chai et al. (2022)

About the Dataset

The data employed in this study is wide ranging mobile app users' behavior, demographics, and psychological traits. It is arranged to enable analysis of the use behavior of app users in relation to digital control and perception of privacy.

Demographics comprise age, gender, nationality, occupation, and level of education. Use of apps is monitored by broad categories of app class e.g., social networking, gaming, finance, lifestyle, and productivity and provides information regarding activity on the

internet. Technical metadata like browser and phone model are monitored as well to provide context for access patterns at the device level.

Personality is assessed on dimensions of empirically established psychological models, and the Big Five is one among these. They are communicated in terms of specific behavioral adjectives like "Extraverted, enthusiastic," "Critical, quarrelsome," and "Calm, emotionally stable," so that users can enjoy nuanced disposition insight.

Two additional characteristics Data Control Level and Ownership Belief are assessing users' perceptions of control over their data and belief about who owns their data. They are quantified as numeric levels and are vital indicators in assessing personal data autonomy.

This data allows for testing and development of forecasting models (e.g., Random Forest classifiers) to detect low perceived control users, and allows clustering techniques to detect behavioral and psychological clusters. It is particularly well suited to examine ethical concerns in digital design, including transparency of consent and agency over data.

Methodology

While examining self reporting mobile device usage and well being, we pursued a systematic data science workflow involving data wrangling, statistical modeling, visualization, and predictive modeling. The rest of this section summarizes the main methods of drawing meaningful inferences from data.

- **Data Cleaning and Preprocessing:** The data were gathered and that included demographic, behavioral, and psychological items. Raw responses were standardized and cleaned. Text responses were mapped to numbers using value mapping and regular expressions. Scales like Total App Usage were calculated by aggregating response across 23 app related questions, and Control Gap was the absolute difference between a user's consent level and ownership belief (Consent Level Ownership Belief). Age values were sampled and binned in certain age bins.

- **Exploratory Data Analysis (EDA):** We employed histograms, bar charts, and

boxplots for statistical analysis of trends. This was conducted by comparing variance of Control Gap values for age groups, as well as personality dimensions and app usage. For instance, younger user groups had more dispersed distribution of Control Gap values compared to older users, who gave more middle range ratings. Personality dimensions were also graphed against age in a bid to establish trends in behavior.

- **Correlation Analysis:** We had computed correlation matrices to identify directions and sizes of association among variables. It was found that personality types like "anxious" and "disorganized" had positive correlation with higher values of Control Gap. Types like "dependable" and "calm" were more common in low Control Gap usage.

- **Machine Learning Models:** Two classifiers, Random Forest and Logistic Regression, were trained to identify users likely to have high Control Gap scores. Both used personality features, age group, and application usage features. Random Forest also enabled identifying the most important features with importance scores. The models were very good at identifying their role in user control perception.

- **Clustering and Segmentation:** We applied K-means clustering to categorize users according to behavior and psychological traits. The unsupervised method generated user groups like "high usage, high anxiety, low control" or "low usage, reliable, high control," and investigated which categories of users are most disempowered on the internet. Through the above methods combined, analysis provides a rich, multi faceted map of mobile phone use and its impact on perceived control and well being.

Findings and Graph Insights

Some of the results consist of some conclusions made for users' perceived control over their behavior, personality, and demographic based data. These are the most compelling visualizations shared here that are explained and correlated with user wellness patterns and digital resource usage patterns in general.

Control Gap Distribution: One of the most significant findings from this case study is the seeming difference in Control Gap scores by age group. The Control Gap is the gap between how much control individuals think they have over their own information, and the actual permissions they've surrendered through mobile apps. As can be seen from the bar chart, this gap increases with age. Users in the age bracket 50-60 demonstrate the highest Control Gap, meaning they may overestimate data control more than other younger age groups.

This is a worrying trend. Older people are not aware of how to configure the privacy settings on modern apps, or they don't review app permissions on a regular basis. Users in their 20s, however, have the lowest Control Gap, perhaps due to their higher familiarity with technology and the way digital consent works. But within this demographic as well, the gap still exists showing that digital privacy myths are widespread.

These results suggest the need for more transparent and age suitable models of consent. If consumers are deceived regarding how their information is being used, especially older adults, it can lead to confusion, exposure, and distrust. The evidence is in favor of the idea that more explicit disclosures and simpler to use privacy settings can bridge this gap and enable users of all ages to feel more secure about their online privacy. .Goldberg (2013)

Personality Traits and Age Based Differences: Yet another graph, Figure 2, calculates average personality trait scores by age groups. Figure 2 is used to indicate how emotional and behavioral tendencies are influenced by age and how it relates to digital control. As an example, personality traits "dependable" and "calm" were found to be always high in the case of old users, and these users also had smaller Control Gaps. Younger respondents also scored more highly on "anxious" and "disorganized," consistent with larger Control Gaps elsewhere in the study.

This would imply psychological stability as a factor in how people think about and engage with digital privacy might be at play. Also, the trends do have the effect of moving the validity of personality based traits further along in predictive models. How these traits influence behavior is perhaps something that is helpful to app developers and data scientists

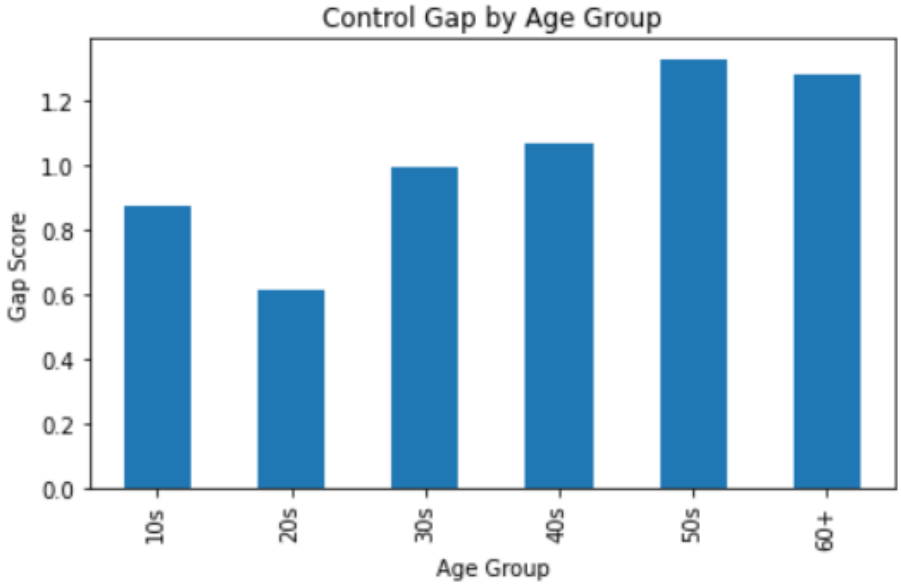

Figure 1

Control Gap Distribution

in terms of customizing privacy education tools to be more appropriate for those who are more emotionally or cognitively vulnerable.

Together, these visual data confirm that personality and user behavior must be accounted for in any discussion of online wellness and privacy. Control is not so much a technical issue it's also a social and psychological one. Lutz & Hoffmann (2017)

Ethical Considerations

As growing numbers of mobile applications process, transmit, and devour huge quantities of personal information, ethics of participating in internet based action in online public space have become more pressing and complicated. This public health use case study of mobile phone use outlines a series of significant issues involving informed consent, data literacy, and psychological impact especially on susceptible subgroups of youth and personality.

One of the largest ethical issues this study entails is the Control Gap between user consent and knowledge. A broad Control Gap would imply that users are providing consent to data usage without complete knowledge of the outcome. It challenges the legitimacy of

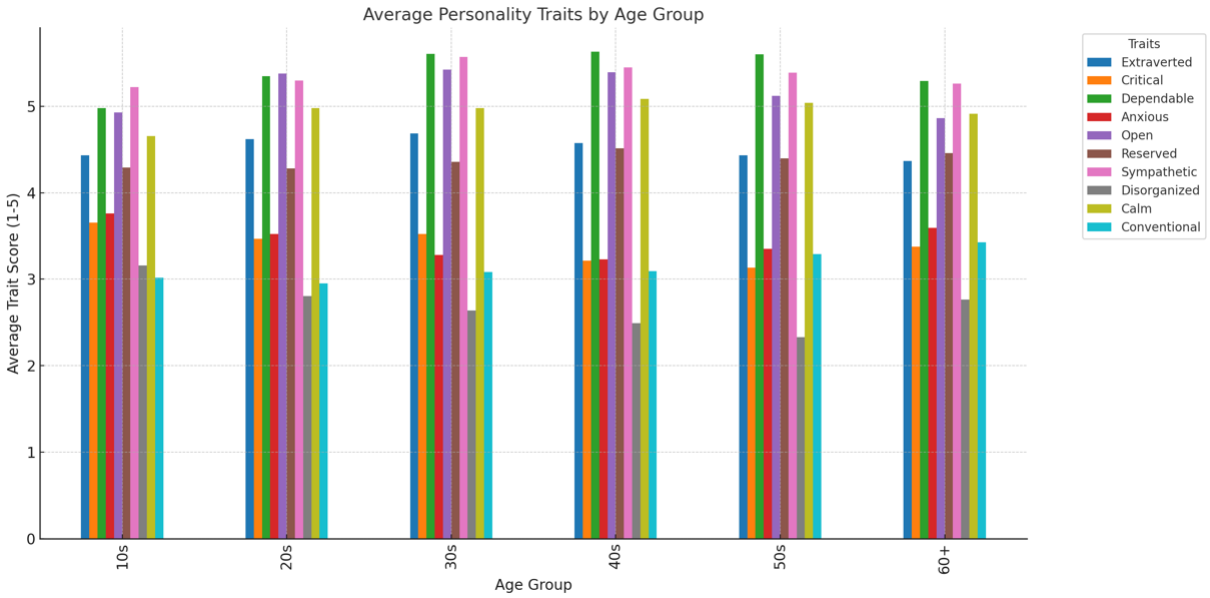

Figure 2

Average Personality Traits by Age Group.

consent in the internet era. If the users do not know what they are agreeing to—or they are being presented with amazing or deceptive user interface designs (more aptly referred to as "dark patterns") then their consent is not even voluntary and informed.

Equity of data is also an ethical concern. Results show that certain types of users i.e., young, high anxiety level, or predisposition to disorder users are more vulnerable to low felt control of data in the virtual world. These users do not have sufficient protection from data abuse, e.g., by low trust in permission checking or by excessive use of mobile apps without any regard to privacy exchange. This is a justice and fairness issue in the Internet, as not all users who use it are completely capable of protecting their information.

The book also explores the ethic of beneficence in artifact creation. The platform operators and the developers do not necessarily need to harm, but must do so up to a certain point by actively purposefully creating user enablement interfaces within a view of digital wellness. The expense of effect on disempowerment online, either in the situation of controls being out of the users' power or in the situation of not wanting to initiate a chilling avalanche of permissions, can devalue credibility online and cause emotional exhaustion.

Finally, from a data science standpoint, there is a moral obligation to utilize predictive models and behavior segments for the benefit of the public. Low perceived-control user identification does not have to be taken further to target or track users for advertisements. Instead, they can be utilized to enable interventions like personalized privacy suggestions, better language in consent, or simpler controls to allow users greater control over their data.

Ethics in AI and data science must be all about moving forward with user dignity, transparency, and fairness regardless of anything else, especially when digital tech is at the middle of our social and emotional life.Ali et al. (2019)Malomo & Sena (2017)

Conclusion

This case study illustrates the richness of meaning of mobile phone use, not only for digital privacy, but for people's health and wellbeing as well. In demystifying and defining the Control Gap, we have identified a broad gap between what people believe they know about their data and what they actually permit. It's not a technical gap alone, but it's psychological too and this results in confusion and mistrust in internet systems.

Statistical processing demonstrated that younger interviewees or even individuals with specific characteristics such as high anxiety or being disorganized do not have control over their online information. In contrast, overuse of an app is not related to greater digital literacy users of most mobile apps are sometimes just those who are least aware of their right to their own information. These results represent a clear call for context sensitive intervention to facilitate more well-informed digital decisions for the users. Finally, the research once more suggests the centrality of digital openness and autonomy as a public good dimension. With the advent of today's networked world, there is a necessity to care for and respond to the psychological effect of the application of mobile technology not only for the user but also for the digital world.

References

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How facebook's ad delivery can lead to biased outcomes. *Proceedings of the ACM on human-computer interaction*, *3*(CSCW), 1–30.

Berr, K. (2019). *Slaves to our screens?: A critical approach to self-regulation of smartphone use at the example of apple's screen time feature.*

Chai, T., Li, J., Prasad, S., Lu, Q., & Zhang, Z. (2022). Shape-driven lightweight cnn for finger-vein biometrics. *Journal of Information Security and Applications*, *67*, 103211.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. *arXiv preprint arXiv:1808.05096*.

GDPR, E. (2018). *General data protection regulation (gdpr).* Intersoft Consulting.

Goldberg, L. R. (2013). An alternative "description of personality": The big-five factor structure. In *Personality and personality disorders* (pp. 34–47). Routledge.

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2018). The privacy policy landscape after the gdpr. *arXiv preprint arXiv:1809.08396*.

Lisowski, J. N. (2023). California data privacy law and automated decision-making. *J. Corp. L.*, *49*, 701.

Lutz, C., & Hoffmann, C. P. (2017). The dark side of online participation: exploring non-, passive and negative participation. *Information, Communication & Society*, *20*(6), 876–897.

Malgieri, G., & Custers, B. (2018). Pricing privacy–the right to know the value of your personal data. *Computer Law & Security Review*, *34*(2), 289–303.

Malomo, F., & Sena, V. (2017). Data intelligence for local government? assessing the benefits and barriers to use of big data in the public sector. *Policy & Internet*, *9*(1), 7–27.

Rizk, H., Abbas, M., & Youssef, M. (2021). Device-independent cellular-based indoor location tracking using deep learning. *Pervasive and Mobile Computing*, *75*, 101420.