On the Elicitation of Privacy and Ethics Preferences of Mobile Users

Patrizio Migliarini
patrizio.migliarini@graduate.univaq.it
University of L'Aquila
L'Aquila, Italy

Gian Luca Scoccia
gianluca.scoccia@univaq.it
University of L'Aquila
L'Aquila, Italy

Marco Autili
marco.autili@univaq.it
University of L'Aquila
L'Aquila, Italy

Paola Inverardi
paola.inverardi@univaq.it
University of L'Aquila
L'Aquila, Italy

ABSTRACT

Nowadays, mobile users are constantly being connected and increasingly asked to express their personal preferences in the digital world. User preferences deal with simple device settings options, like notification alarms, as well as relevant ethical choices relating to the user behavior, privacy ones included (e.g., concerning the unauthorized disclosure and mining of personal data, as well as the access to restricted resources). All these preferences define the user, they are the building blocks of her digital identity and will be increasingly important given the growing rise of autonomous technologies and their ethical implications. The settings that enable these preferences are often hard to locate and hard to understand, even in popular apps and operating systems. Moreover, they can expose privacy, be employed for profiling or exploited for malicious activities. In this landscape, we devise the introduction of a *Personal Preferences Automation Module* (PPAM) capable of automatically inferring, applying and enforcing user choices in multiple scenarios ranging from speeding up simple time consuming tasks, to managing sensitive ethical choices. The wide range of sensors and devices that can be found in the mobile domain makes it a privileged context in which to employ the proposed module. In this paper, we present two application scenarios and describe the proposed approach at work on them.

KEYWORDS

Personal preferences, Privacy, Ethics, Mobile devices.

ACM Reference Format:
Patrizio Migliarini, Gian Luca Scoccia, Marco Autili, and Paola Inverardi. 2020. On the Elicitation of Privacy and Ethics Preferences of Mobile Users. In *IEEE/ACM 7th International Conference on Mobile Software Engineering and Systems (MOBILESoft '20), October 5–6, 2020, Seoul, Republic of Korea.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3387905.3388610

MOBILESoft '20, October 5–6, 2020, Seoul, Republic of Korea

ACM ISBN 978-1-4503-7959-5/20/05…$15.00
https://doi.org/10.1145/3387905.3388610

1 INTRODUCTION

Mobile devices are always in the hands or pockets of almost 4 billion users worldwide [34]. Mobile users continuously interact with the digital world to the point that it no longer makes sense to talk about online and offline situations. Following [23], we call today digital involvement an *onlife* experience.

Digital interactions are "disciplined" by user-specified preferences, which often affects the privacy and ethics sphere of the user herself [9]. As a consequence, ethical issues – privacy ones included (e.g., unauthorized disclosure and mining of personal data, access to restricted resources) – are emerging as matters of utmost concern as they impact on the moral rights of each human being and affect the social, economic, and political spheres [1, 13, 20].

Comparing today number of user-specified preferences settings available in any major mobile operating systems to the ones available five or ten years ago, we can easily grasp how relevant user preferences became in software design. Through preferences management, developers and builders emphasize the device capabilities while chasing compliance to the legislation, in turn, increasingly sensitive to the evolving topics of privacy and ethics [31]. Preferences are not limited to general system settings but can be expressed in and for any single app installed in the user's device. Furthermore, any website can, potentially, keep track of users' preferences with profiling technologies [19].

With over 5 million apps in the major app stores, downloaded 204 billions of times [5], the management of preferences has now become a main topic in today user experience [4]. To effectively express preferences and configure settings on privacy, security, and ethics while using connected devices is time consuming, not clear and not easy to do [3, 15, 22]. Vendors are encouraging developers to avoid or delay asking preferences, trying instead to *"Infer what you can from the system"* [7].

Our bold vision is to create an independent system to be queried by, e.g., apps, web sites, operating systems any time a preference is required. Starting from general user profiles, which include ethical and behavioral aspects, we build a fine-grained *User Model* to be exploited by the system to understand and actuate preferences without the intervention of the and user. The User Model is continuously personalized and tailored to the individual user through systematic, run-time feedback and a dedicated feedback interface. As schematized in Figure 1, we consider a Personal Preferences Automation Module (PPAM) as the evolution of the today preferences

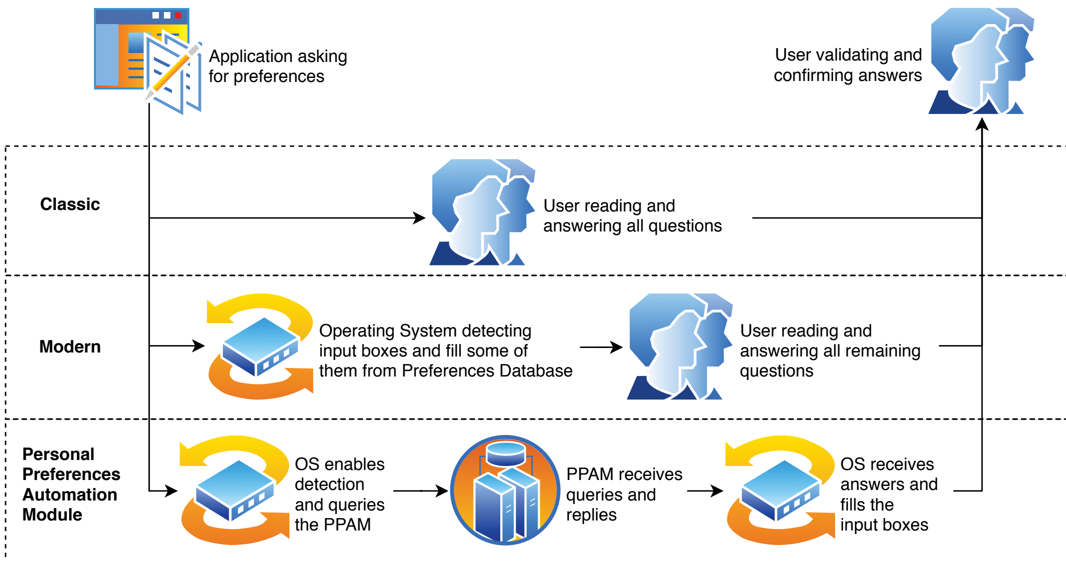

Figure 1: Diagrams of the preferences request flow for classic, modern and Personal Preferences Automation Module

management that started from very basic per-app settings (classic preferences management of years ago) to operating system-level enforcement (like the one found in recent iOS [36], iPadOS [35] and Android [18]). Similarly to what the Trusted Platform Module [11] has been for the evolution of cryptography, our system could be integrated as middleware in modern computing platforms [9].

Considering the variety of input data required to tailor a personalized User Model, including the emotional and biometric ones [17], the mobile domain is particularly suited for our vision, due to its sensors-rich nature. Modern mobile devices are in fact equipped with audiovisual (e.g., high resolution camera, microphone), biometric (e.g., heart beat monitor, galvanic skin response [21]) and motion sensors (e.g., gyroscope, accelerometer) which may be of use.

2 THE VISION

The system we are designing shall interface with any software that, interacting with the user, will ask for a choice and, acting on her behalf, will express her preferences. It should act hence automating the elicitation process while enforcing her preferences as if she were asked explicitly. The goal of the system is to significantly reduce the effort required to the user from managing her preferences in an increasingly digitalized world, and to provide her with the means to express her choices in situations where the number of questions makes the effort required to reply unaffordable. Furthermore, it will permit to speed up the process and to prevent possible errors. Indeed, automation has substantially reduced the cost of asking standardized questions to multiple individuals; conversely, the cost to formulate an answer remains constant [12].

The proposed system relies on an internal model of the user's ethics and beliefs to answer requests on her behalf. Starting from a base ethical model, assigned to the user on the basis of his personal traits and an initial training (e.g., a short questionnaire, gamification [29]), it is continuously refined and better tailored to the individual user during the PPAM system lifetime. To this end, we leverage two sources of feedback: an explicit feedback interface provided to the user and the rich variety of sensors available on modern mobile devices, to factor in contextual, biometric and sensor data harvested in situations where the user ethic is called into action.

The workflow of the PPAM system is displayed in Figure 2 and it is conceptually divided in three phases: *Triggering*, *Reasoning* and *Synthesizing*. The first phase concerns the activation of the system, which is called into action when, while interacting with her device, the user is asked to provide some ethics-relevant information (e.g., while filling an input form). At this point, the PPAM is activated, either automatically triggered by context, sensors and bio-metric data, or manually by the user (e.g., by pressing a button integrated with the on-screen keyboard). Once the module is active, the Reasoning phase begins. The Inferential Engine takes into consideration the set of rules and laws preset by authorities ("Hard Ethics" [9, 24, 30]), the historical database of user preferences, the user's ethical model references on "Soft Ethics" and the available data (i.e., contextual and sensors data) and evaluates the request made to the user. As a result of the evaluation, the ethical dimension(s) affected by the request (e.g., environmentalism, selfishness) is identified and handed over to the Input Generator, thus initiating the Synthesizing phase. The Generator queries the User Model to retrieve the previously assessed user's belief for the identified dimension(s) and produces an answer to the request (e.g., values for fields in the case of a form). Once the input data is transmitted to fill the input boxes, the user may visualise, confirm and edit it before submission. Afterward, submitted data will be used to update the User Model and refine the Ethical Model, and will be saved in the Historical Database for future reference and inference.

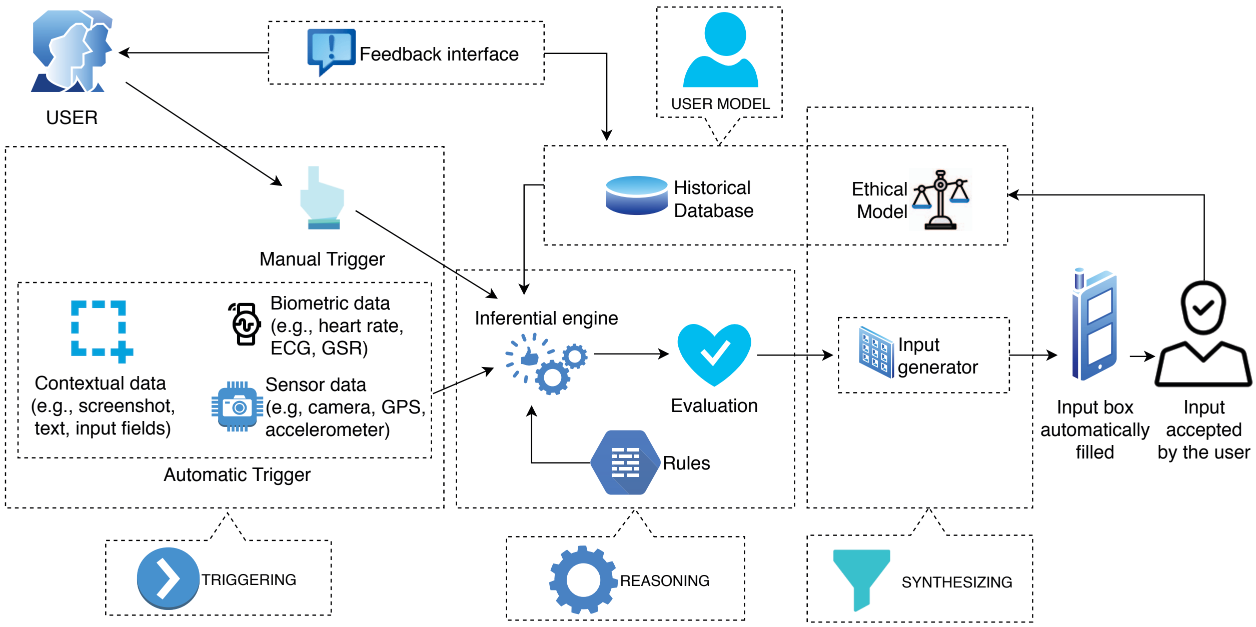

Figure 2: Diagram of the Personal Preferences Automation Module workflow

By means of simple controls, the Feedback Interface in the system enables the user to interact with the User Model, examine and review the automatically inferred beliefs and decide whether certain assessments were accurate or relevant enough. This interface can be inspired by existing reporting tools (e.g., Apple Screen Time [8] or Google Digital Wellbeing [26]), and it is introduced to keep the user in control [29] and fulfill the *"right to explanation"* [16, 25], which is particularly relevant when dealing with users' ethics.

In the following, two illustrative examples highlight potential applications of PPAM and its novelty.

Example 1 - Consider a user that, by means of a flight reservation app, wants to book a flight ticket. During the process, she is asked to input personal data (e.g., name, surname, nationality) and travel details (e.g., departure time window, baggage type). Finally, before completing the purchase, she is asked if she is willing to pay a *decarbonization tax*, i.e., a small fee that will serve to offset the impact of carbon emissions caused by the flight. From an ethical perspective, asking the user to pay this tax is equivalent to asking her if she is willing to sacrifice some immediate utility (the fee) in exchange for a less tangible and shared societal benefit (the reduction in pollution). Mechanisms that (semi-)automate the insertion of non ethical-relevant information are either already readily available, as in the case of personal data (e.g., Apple ID [6] data in Apple iOS or Google Account [27] in Android), or acquirable (e.g., departure time window could be inferred from the user calendar app, baggage type from the length of the flight). On the contrary, there is no mechanism to automate the decision about the decarbonization tax, as the user's willingness to accept it depends on her own ethical traits, behavior and context (e.g., how selfish and how keen on the environment she is). PPAM fills this gap, providing a solution to automate the insertion of ethical information akin to what it is already available for standard one.

Example 2 - A second example of application of PPAM is an automated queuing system of a post office ticketing service. During the process of remotely booking to collect a parcel from the post office, the user is asked to input multiple information like personal data, tracking number of the shipping, a time frame for her booking, etc. She may also be asked if she is willing to give way to other users with special needs (e.g., to pregnant women) who booked after her, and that could, therefore, cause a short delay compared to the exact booking time. In this example, from an ethical perspective, asking the user to possibly increase her waiting time is equivalent to asking her if she is willing to sacrifice some immediate utility (the time) in exchange for a less tangible and shared social benefit (the time saved by others). As for the previous example, (semi-)automated insertion of some information is possible (e.g., tracking number of the shipping from an email) while the willingness to sacrifice some time in favor of other users depends on her own ethics, and not currently available. Also in this case, PPAM provides a context-aware solution to automate this ethical-relevant choice, by relying on the User Model.

3 WHY IS IT NEW?

The main and brand new feature of this system is the ability to synthesize a user model from which to infer user preferences, including the ethical ones, and automatically apply them whenever it is of help to the user (e.g., fast-paced situation, complex sets of questions, etc.). To the best of our knowledge, this is a first attempt to model and to include ethical aspects in preference management, allowing it to handle a broader variety of requests. Unlike the passive history-based present systems (e.g., Apple ID [6] for iOS and

Google Account [27] for Android), PPAM proactively enforces user preferences when faced with requests. In addition, due to the sensitive nature of this novel ethical dimension, it is independent of the underlying operating system and not integrated with users' accounts. This permits to keep the user in charge of her data without intermediaries and to reduce unwanted profiling further enabling straightforward and easy preferences management.

Considering the plurality of interests at stake, we envision that, past the prototype stage, our system may be designed, engineered and managed by a consortium, composed of both industrial and academic partners. This vision is inspired by the Trusted Computing Group [28], a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global specifications and standards for interoperable trusted computing platforms. Similarly, a PPAM Management Group would be in charge of developing, spreading and maintaining specifications and standards related to the Personal Preferences Automation Module, so as to regulate the profiling, the access to and the exchange of the User Model among trusted parties.

4 THE RISKS

Our vision puts forward a set of relevant challenges. The experiment of Agrawal and colleagues [10] provided strong clues about the multi-faceted nature of ethical judgments, where even the strongest preferences shared by many users show to be affected by substantial cultural variations. Our vision adds a degree of complexity since it aims at modeling and acting on the ethics of each own uses. A second challenge is to obtain enough information to correctly assess and model the user's assumptions. In this regard, not only we are limited by the accuracy and amount of available sensors, but we must preliminary understand what are the situations in which ethical judgment is called into action, what dimensions of it are affected and to what extent. We plan on designing and conducting extensive user experiments in this regard.

It is important to also keep in mind the possible misuses that could be made of PPAM. Similarly to the behavior [19, 37], the user's ethics is a piece of strictly personal information. Its collection could be appealing to those digital actors that have an interest in profiling the user's behavior and attitudes, to exert some influence on it [14] or to maximize product revenues [32]. Hence, to deal with privacy and security concerns, we envision an open-source implementation of the system, possibly managed by a consortium of both industrial and academic partners (as described in Section 3). Relying on an open architecture introduces fundamental transparency in the system and mitigates possible exploits of the module against the users' privacy.

Considering the relevance and frequency of cyber-attacks based on deception against the user, we imagine that this type of attack can also be designed against PPAM. When launched against the end user, the mitigation of these attacks is completely delegated to the level of attention and training of the user who should notice and avoid a potential scam [12]. By using PPAM, the user is enabled with an additional level of protection derived from the possibility of automatic threats data sharing between PPAM users. Similarly to modern antivirus software, the PPAM architecture can provide a sharing network for potential dangers and scams, allowing the user to automatically take advantage of the experience of the users other than a managed threats database.

It is undoubtedly a challenge to design a system to manage ethical preferences considering that they derive from multiple factors (e.g., cultural, social, contextual), not common to all and not always generalizable. Precisely for this reason, we see as an added value promoting the participation in the consortium of institutions able to guarantee the plurality of expressions and representativeness of cultures, ethnic groups, beliefs, theoretical principles.

The integration of PPAM (initially software but with the prospect of becoming embedded software to be specialized and optimized for the particular target hardware) that interfaces with the operating system rather than with individual applications, should respond effectively and efficiently to the need to interface with the enormous diversity of mobile applications available to date, considering instead the small number of operating systems currently available.

5 NEXT STEPS

The development of the Personal Preferences Automation Module requires, as first, the consolidation of the theoretical foundations, the underlying basis and principles, on which we build the preliminary user models of ethical preferences. This will be achieved through user studies, involving participants from different cultures, age, sex, educational level, etc. Users will be asked about ethical-relevant questions and they will be proposed to take part of ad-hoc experiments whose design and execution are inspired by the Moral Machine Experiment [10]. The goal of these experiments is the definition of the base ethical models that would be the starting point of the process for synthesizing the user model. The base user models will also be used to define the context analysis in conjunction with bio-metrical sensors analysis to trigger the reasoning process. This process will lead to the building of a fine-grained and personally-refined model of the user that will adopt the PPAM. We will continue investigating the use of off-the-shelf bio-metrical sensors equipped products, like smartwatch and smartbands, to develop an efficient triggering and analysis implementation based on user actions and reactions. An efficient inferential engine will be the key factor for the success of the system in order to correctly evaluate the possible response to be passed to the Input Generator. Our approach aims to be as white box as possible in order to fulfill the emerging normative for which *"explicability is crucial for building and maintaining users trust in AI systems"* [29]. The development of the inferential engine will involve the consideration of the rules, norms and laws that will constitute the "hard ethics" [9, 24] component of the reasoning, to fulfill compliance with applicable laws and regulations [29].

Another effort will be devoted to the development of the input generation that follows the evaluation from the inference engine. For that purpose, it is necessary to develop a software able to analyze the multi-faceted types of available input and synthesize an answer considering the inference engine evaluation.

The feedback interface is also essential to enable the user to review, change and express her judgments about the User Model in an easy and intuitive way. Here, we plan to adopt best practices of user interface development [33] and user-centered-design [2] methods.

REFERENCES

[1] 2018. European Group on Ethics in Science and New Technologies. Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems. https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.

[2] Chadia Abras, Diane Maloney-Krichmar, Jenny Preece, et al. 2004. User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications* 37, 4 (2004), 445–456.

[3] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, and et al. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (Aug. 2017), 41 pages.

[4] Christoph Anderson, Isabel Fernanda Hübener, Ann-Kathrin Seipp, Sandra Ohly, Klaus David, and Veljko Pejovic. 2018. A Survey of Attention Management Systems in Ubiquitous Computing Environments. *IMWUT* 2, 2 (2018), 58:1–58:27.

[5] APP Annie. 2020. The State of Mobile in 2020: The Key Stats You Need to Know. https://www.appannie.com/go/state-of-mobile-2020

[6] Apple. 2020. Apple ID. https://appleid.apple.com

[7] Apple. 2020. Human Interface Guidelines. https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/settings/

[8] Apple. 2020. Screen Time. https://support.apple.com/en-us/HT208982

[9] Marco Autili, Davide Di Ruscio, Paola Inverardi, Patrizio Pelliccione, and Massimo Tivoli. 2019. A Software Exoskeleton to Protect and Support Citizen's Ethics and Privacy in the Digital World. *IEEE Access* 7 (2019), 62011–62021.

[10] Edmond Awad, Sohan Dsouza, Richard Kim, Jonathan Schulz, Joseph Henrich, Azim Shariff, Jean-François Bonnefon, and Iyad Rahwan. 2018. The moral machine experiment. *Nature* 563, 7729 (2018), 59–64.

[11] Sundeep Bajikar. 2002. Trusted platform module (tpm) based security on notebook pcs-white paper. *Mobile Platforms Group Intel Corporation* (2002), 1–20.

[12] Rainer Böhme and Jens Grossklags. 2011. The security cost of cheap user interaction. In *Proceedings of the 2011 New Security Paradigms Workshop*. ACM, 67–82.

[13] J. Peter Burgess, L. Floridi, A. Pols, and J. van den Hoven. 2018. Towards a digital ethics - EDPS Ethics Advisory Group. https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

[14] Carole Cadwalladr and Emma Graham-Harrison. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The guardian* 17 (2018), 22.

[15] Yi Chen, Mingming Zha, Nan Zhang, Dandan Xu, Qianqian Zhao, Xuan Feng, Kan Yuan, Fnu Suya, Yuan Tian, Kai Chen, et al. 2019. Demystifying Hidden Privacy Settings in Mobile Apps. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 570–586.

[16] European Commission. [n.d.]. *Statement on artficial intelligence, robotics and 'autonomous' systems.* https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

[17] Stefania Costantini, Giovanni De Gasperis, and Patrizio Migliarini. 2019. Multi-agent System Engineering for Emphatic Human-Robot Interaction. In *2019 IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE)*. IEEE, 36–42.

[18] Android Developers. [n.d.]. *Android Settings Menu.* https://source.android.com/devices/tech/settings/

[19] Peter Eckersley. 2010. How unique is your web browser?. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 1–18.

[20] EDPS. 2015. Leading by example, The EDPS Strategy 2015-2019. https://edps.europa.eu/sites/edp/files/publication/15-07-30_strategy_2015_2019_update_en.pdf.

[21] Empatica. 2020. Embrace2. https://www.empatica.com/embrace2/

[22] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David A. Wagner. 2011. Android permissions demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011*. 627–638.

[23] Luciano Floridi. 2015. Luciano Floridi—Commentary on the Onlife Manifesto. In *The onlife manifesto*. Springer, Cham, 21–23.

[24] Luciano Floridi. 2018. Soft Ethics and the Governance of the Digital. *Philosophy & Technology* 31, 1 (2018), 1–8.

[25] Bryce Goodman and Seth Flaxman. 2017. European Union regulations on algorithmic decision-making and a "right to explanation". *AI magazine* 38, 3 (2017), 50–57.

[26] Google. 2020. Digital Wellbeing. https://wellbeing.google/

[27] Google. 2020. Google Account. https://myaccount.google.com

[28] Trusted Computing Group. 2020. About TCG. https://trustedcomputinggroup.org/about/

[29] AI Hleg. 2019. Ethics guidelines for trustworthy AI. *B-1049 Brussels* (2019).

[30] Paola Inverardi. 2019. Ethics and Privacy in Autonomous Systems A Software Exoskeleton to Empower the User. In *International Workshop on Software Engineering for Resilient Systems*. Springer, 3–8.

[31] Paola Inverardi. 2019. The European perspective on responsible computing. *Commun. ACM* 62, 4 (2019), 64–64.

[32] Ganesh Iyer, David Soberman, and J Miguel Villas-Boas. 2005. The targeting of advertising. *Marketing Science* 24, 3 (2005), 461–476.

[33] Brenda Laurel and S Joy Mountford. 1990. *The art of human-computer interface design.* Addison-Wesley Longman Publishing Co., Inc.

[34] Statista. 2020. Number of smartphone users worldwide from 2016 to 2021. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[35] Apple Support. 2020. *Change common iPad settings.* https://support.apple.com/guide/ipad/change-common-settings-ipad79520415/ipados

[36] Apple Support. 2020. *Change common iPhone settings.* https://support.apple.com/guide/iphone/change-common-settings-iph70825e5ae/ios

[37] Wan-Shiou Yang, Jia-Ben Dia, Hung-Chi Cheng, and Hsing-Tzu Lin. 2006. Mining social networks for targeted advertising. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, Vol. 6. IEEE, 137a–137a.