information

Communication

Human Autonomy in the Era of Augmented Reality—A Roadmap for Future Work

David Harborth

Chair of Mobile Business and Multilateral Security, Goethe University Frankfurt, Frankfurt am Main, 60323 Frankfurt, Germany; david.harborth@m-chair.de

Abstract: Augmented reality (AR) has found application in online games, social media, interior design, and other services since the success of the smartphone game Pokémon Go in 2016. With recent news on the metaverse and the AR cloud, the contexts in which the technology is used become more and more ubiquitous. This is problematic, since AR requires various different sensors gathering real-time, context-specific personal information about the users, causing more severe and new privacy threats compared to other technologies. These threats can have adverse consequences on information self-determination and the freedom of choice and, thus, need to be investigated as long as AR is still shapeable. This communication paper takes on a bird's eye perspective and considers the ethical concept of autonomy as the core principle to derive recommendations and measures to ensure autonomy. These principles are supposed to guide future work on AR suggested in this article, which is strongly needed in order to end up with privacy-friendly AR technologies in the future.

Keywords: augmented reality; information privacy; informational self-determination; behavior modification; ethics of technologies

Citation: Harborth, D. Human Autonomy in the Era of Augmented Reality—A Roadmap for Future Work. *Information* **2022**, *13*, 289. https://doi.org/10.3390/info13060289

Academic Editors: Ramon Fabregat, Jorge Bacca-Acosta and N.D. Duque-Mendez

Received: 6 May 2022
Accepted: 4 June 2022
Published: 7 June 2022

1. Introduction and Definition of the Problem Space

The market on immersive technologies, such as augmented reality (AR) or virtual reality (VR), is facing an immense change with respect to competitors and technological developments. The market for AR technologies in general was worth $1.8 billion in 2018, $3.5 billion in 2019, and is expected to increase in value to $18 billion by 2023 [1]. In addition, a quarter of the US population, 72.8 million people, used AR at least once a month in 2019. A recent study estimated that this number will increase to 95.1 million people in 2022 (representing 28.6% of the whole US population) [2]. However, technologies such as AR and VR are embedded within a larger context that has seen its hype in the recent rebranding of Facebook into Meta in late 2021 [3], namely, the so-called metaverse. The metaverse basically represents a second layer on top of the real world in which every individual joins with her or his avatar (basically a digital twin of the real world). AR and VR technologies are one of the key technologies to bring the metaverse to individuals' homes, while AR plays a special role in this development as its possibilities are less limited than those of VR devices [4]. Furthermore, Meta is not the only company that aims at creating a second digital layer on top of the real world. Niantic, a startup founded under the umbrella of Google [5], announced the beta version of its AR cloud called *Lightship* in November 2021 [6]. These developments are appearing to be more relevant in light of the interest of other big technology companies such as Apple. For example, Tim Cook, CEO of Apple, implied in 2016 that AR might become as ubiquitous and important as the smartphone today:

"AR is going to take a while, because there are some really hard technology challenges there. But it will happen, it will happen in a big way, and we will wonder when it does, how we ever lived without it. Like we wonder how we lived without our phone today" [7].

Based on these insights on the relative importance of the type of immersive technology, this work will primarily focus on AR in the following discussion. All of the changes in this

current (AR) market make it imperative for us researchers to investigate these technologies as early as possible in order to ensure that they do not harm our societal and democratic developments. I argue that the sole investigation of the positive potential of these technologies is not sufficient to propose necessary changes in technologies to developers and policy makers. Rather, we need to look at the "dark side" of the developments. Potential issues for AR include a constant distraction from the real world, technostress [8,9], the possible feelings of humans that they are "robots" controlled by the technology, and, finally, privacy and security issues.

This work focuses on privacy, since this is one the most pressing issues of our time in the context of AR with respect to individual self-determination and consumer protection rights. On the one hand, individuals could potentially substitute their smartphone and wear these devices at all time, constantly processing the environment around them. All of the sensor data of the devices (camera, eye-tracking, etc.) would be a potential source of so far unknown multidimensional privacy risks that are more severe than those known from prior technologies. On the other hand, technology companies like Alphabet (Google), Meta (Facebook), and Amazon dominate a large share of the market for personal data in the world [10]. The primary business model of these companies consists of collecting and processing personal information (Google, Meta) or it increasingly tends to move towards this kind of revenue source (Amazon). In light of the success of these "surveillance capitalists" [11], businesses all over the world continuously started to change their business models to rely on the rationale of "big data" and gather as much personal information as possible [12]. Oftentimes, the set goal in their cases is not only to use personal information in order to improve products or provide products that are tailored to certain target groups, but rather to modify the behavior towards the desired outcome of the companies [11]. Thus, privacy issues can lead to risking individuals' self-determination. The logic of behavior modification might sound like a future dystopian possibility that does not have any relevance in research and development today; however, this risk is now ample due to the recent developments regarding the metaverse, the AR cloud, and the immersive technologies themselves as they enable companies in previously unknown manners to gather information on the human behavior and act accordingly based on it.

One of the most profound examples of this logic can be observed for the MAR app Pokémon Go. The smartphone game was developed by the previously named company Niantic, which earned USD 900 million in 2019 in player spending with the game Pokémon Go [13]. However, there is another substantial stream of revenue for the company, namely, the use of behavior modification to guide players to sponsored "PokeStops" where they can get special perks in the game (e.g., rare Pokémon). For example, these sponsored locations were Starbucks coffee shops or McDonald's branches, which pay Niantic per physical visit of a player. Numbers by late 2017 reported 35,000 sponsored locations with roughly 500 million visits [14]. Augmenting the real world with digital information, as well as consequently following the logic of behavior modification, enabled Niantic to push users—most likely without their knowledge—to these stores in the actual real world and convert information about them into revenue.

This logic of behavior modification is well summarized by John Hanke, CEO of Niantic, and formerly the head of the Geo division of Google who was, among others, responsible for a privacy scandal during the Street View project [15]:

"[...] could the products that they're using cause them to walk a different path, drive a different path, divert from the trajectory that they're normally going to go on? If you could do that through information services that you're offering to people, there's tremendous opportunity there for businesses that might want to change the behavior of people, to get them to go places they wouldn't otherwise go" [16].

I argue that this logic is especially relevant to consider when analyzing a technology like AR, which is perfectly suited to implement this logic of human behavior change due to the variety of sensors of the technology.

Thus, the goal of this communication paper is to (1) elaborate on the risks of behavior modification within the context of AR and differentiate it towards previously known approaches that change the human behavior (nudges), (2) discuss the relation of autonomy, as a guiding principle for all research aimed at ensuring sustainable technological developments, to privacy, and (3) suggest approaches for ensuring autonomy in the era of AR based on prior empirical findings and normative guidelines.

The remainder of the article is structured as follows. Section 2 provides an overview of nudging and differentiates it from behavior modification. Section 3 discusses how privacy issues relate to individual autonomy. Section 4 discusses three potential approaches for protecting autonomy in light of rising privacy risks in the context of AR technologies. Section 5 provides an outlook on the necessary future work to ensure individuals' autonomy in the era of AR.

2. Nudging versus Behavior Modification

As discussed before, behavior modification with technologies like AR occur when companies use that technology and respective user data to modify the behavior of the user towards a desired outcome. It is therefore important to assess to what extent behavior modification differs from related concepts involving the intentional change of the behavior of individuals. One of the most prominent examples is the concept of "nudging", which originates from the work of Thaler and Sunstein [17]. Nudges are defined as "interventions that steer people in particular directions but that also allow them to go their own way" [18]. The applications in which Thaler and Sunstein [15] propose these alterations of individual choice architectures are, by definition, good-natured, such as moving people to a more environmentally friendly behavior [19].

The idea of nudges is to partially overcome the problems associated with individual decision making that is influenced by biases and heuristics [20,21]. For example, such biases and heuristics can influence privacy-related decision making, especially in situations in which individuals use little or no cognitive effort to make the decisions (system 1 decisions) [22,23]. One could argue that interventions in the form of nudges are objectionable, and there is a respective scientific debate on this question and related ethical aspects such as autonomy [18,24,25]. However, one can generally say that an ethical assessment depends on the kind of nudge that is used [18,26]. Cass Sunstein even argues that nudges can "promote people's autonomy—most obviously when they help people to have a better understanding of the facts" [18]. Richard Thaler mentions three features in his plea for "good nudges" in a New York Times article [27]. First, nudges "should be transparent and never misleading". Second, individuals must be given the opportunity to "opt out of the nudge" with as little effort as possible. Third, Thaler argues that the intervention should "improve the welfare of those being nudged" [27].

Besides the design of the nudge itself (e.g., hidden versus obvious, manipulative versus informative), it also matters by whom it is implemented. Nudges are oftentimes tools for governmental regulation [18]. Thus, one can assume a certain level of institutional trust in governmental organizations and there are certain experiences indicating that governments usually follow the three rules for "good nudges" outlined above [27]. The analysis of the institution that does the nudging is especially relevant in the context of this work. I argue that we cannot assume and rely on the general trustworthiness of commercial compared to the case of governmental interventions. This claim is supported by the discussion about nudges and that commercial companies usually hide the interventions and provide as little transparency as possible [26]. In addition, the choice architectures in online environments are oftentimes skewed towards choosing the option that benefits online companies (e.g., the current design of cookie requests on websites, which provides an "accept all" button, but requires multiple clicks for a more granular setting of what should be allowed [28]). Lastly, I assume that commercial companies usually do not have the welfare of the individual in mind, but aim at increasing shareholder value. An example from this work is the mechanism of physically routing players of Pokémon Go to sponsored locations such as

Starbucks or McDonald's branches. Locating relevant spots for players to these sponsored locations does not increase the welfare of the players in an obvious way compared to setting them into a park. However, it generates millions of dollars in revenue for Niantic [14].

In summary, the risks for individuals when using "bad nudges" [27] resemble the work mechanism described in the concept of behavior modification [11]. Thus, I evaluate behavior modification based on the same standards that are used for evaluating nudges. Behavior modification is based on the hidden manipulations of individuals, low levels of transparency, and skewed choice architectures. Furthermore, it cannot be assumed that online companies aim to increase the welfare of the users with their modifications. Therefore, the evaluation of all of the risks of AR and the respective potential for behavior modification leads to the conclusion that there are certain dangers for the individual freedom associated with the current and future use of behavior modification in the context of AR technologies, which need to be considered.

Based on this premise, I discuss the concept of autonomy in the following section. Autonomy is a reoccurring theme in the debate on ethical values related to nudges, and I argue that it is one of the most fundamental values that we should consider in the discussion about technological developments and their impact on individuals. It is important to notice that I do not aim to decide on the necessary degree of autonomy for an individual and on the ultimate respective measures that need to be established to ensure autonomy. However, if we were to consider autonomy to be an important criterion for individual development and a flourishing society, certain technical and regulatory measures would be required to protect autonomy.

3. Autonomy and the Relation to Privacy

Prior work on AR and privacy showed a variety of different privacy risks and their perceived relevance for individuals' privacy concerns in the context of AR technologies (e.g., AR wearables or MAR apps) [29–37]. What is considered to be a violation of privacy is discussed extensively in the literature. It is common knowledge that privacy plays a fundamental role in every human's life, which was fortified by the European Union in 2000 when it stipulated that privacy is a fundamental right according to Article 8 of the EU Charter [38]. However, this mere stipulation does—in the first place—not allow for any concrete measures. One approach to theoretically analyze privacy is the framework of contextual integrity (CI) [39]. Based on the framework of CI, privacy violations can be judged according to certain prevailing norms in the respective society. One important aspect of this evaluation consists of the ethical values that should accompany every discussion about addressing potential privacy threats [40]. A core ethical concept in this context is the autonomy of the individual. As discussed before, autonomy is a common ethical value in the discussion on nudges, which underlines the importance of the concept. I explain the concept of autonomy as well as the relation to privacy in the next subsection in more detail. Afterwards, I use the established premises to elaborate on privacy threats and possible solutions in the context of augmented reality on the supposition that autonomy is the key criterion that "is a normative ideal that is widely shared by thinkers across the political and ideological spectrum" [41].

Autonomy

Autonomy is given if a person can pursue her or his life based on her or his own ideas, causes, and motivations in contrast to being manipulated by the extraneous factors that drive life choices [42]. Considering this definition, autonomy is a kind of antecedent of freedom in a way that freedom is oftentimes associated with a physical act itself, whereas autonomy covers the inner feelings and thoughts of individuals (which are oftentimes formed prior to acting) [43]. This link between thoughts and actions is considered to be less distinct in other research domains in their accounts of autonomy compared to the previously introduced one from the philosophy domain. Beauchamp and Childress consider both thoughts and actions in their definition of autonomy in their book on ethics

in the health profession [44]. For the sake of this essay article, I argue that this distinction, although theoretically important, has no immediate effects on the discussion on privacy in AR technologies and the potential threats to individual autonomy.

However, it is necessary to discuss the general prerequisites of autonomy, since this provides a first step towards understanding the potential measures that help to ensure individual autonomy in the era of augmented reality. There are two theoretical conditions for ensuring autonomy in the literature [41]. First, individuals must be able to expose themselves to a variety of different views and opinions on certain topics instead of only obtaining information through a specific filter associated with a certain worldview. Second, individuals must be able to seclude themselves and go into an "inner dialogue" with themselves or others [41] and elaborate on the aforementioned ideas, causes, and motivations that impact their life choices. These conditions are especially interesting against the backdrop of providing transparency for decisions related to technology use. In addition, it is important to disentangle the relationship between the concept of privacy and autonomy for the consequent discussion. Prior research on autonomy suggests "[...] that privacy is a subset of autonomy" [45]. Based on this, privacy threats of technologies like AR are assumed to negatively influence autonomy and, by extension, ultimately the freedom of individuals if not carefully considered and included in a societal discourse related to the development of such technologies. Such threats can, for example, arise due to a lack of transparency or a manipulation of individual decision rights, which undermines autonomy [46]. This direct relation between threats to users' privacy and autonomy is also shown in other research in the context of online manipulation (e.g., in social networks) [26].

If one compares these insights on autonomy with the current logic of behavior modification, it is striking that the described practices of modifying individual behavior are in stark contrast to the definition of autonomy, since they rely on covertly manipulating individuals to make certain decisions that they would not have made otherwise. This evaluation is supported by the insights from the discussion on "bad nudges" [27]. It became apparent that the practices of behavior modification with AR technologies would not fulfill the criteria of "good nudges", which would make it objectionable with respect to autonomy [18,27]. Therefore, the privacy threats of AR technologies should be addressed as early as possible if autonomy serves as the basis of evaluating these risks and their impact on individuals and society.

4. Approaches to Ensure Autonomy in the Era of AR

I will discuss different approaches for addressing the privacy and autonomy risks of AR technologies in the following subsections. These three pillars are shown in Figure 1.

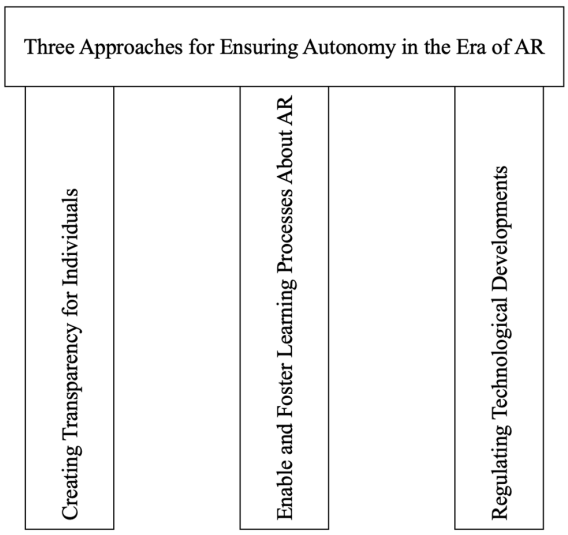

Figure 1. Three approaches for ensuring autonomy in the era of AR.

4.1. Creating Transparency for Individuals

The first approach is based on the assumption that there is a significant information asymmetry between online companies and users [11,47]. This makes it difficult for the user to autonomously form opinions and make consequent decisions. Thus, I argue that new technological approaches that foster information transparency are needed to close the knowledge gap between the two parties. In the context of AR, it became apparent that transparency is a crucial prerequisite for autonomy. Individuals need to be able to make informed decisions with the possibility of taking all necessary facts into account that constitute the benefits and risks. Prior work shows that this is not possible under the current technical regime in the context of MAR applications [48]. Individuals usually have no idea how much information is necessary to deanonymize them. Thus, each newly proposed permission for AR technologies builds upon the idea of creating transparency related to the personal information that is gathered and processed in a specific context at a certain point in time. I argue that this context-dependent provisioning of transparency-enhancing information is one way of addressing the problem of information asymmetry, which is crucial for preserving autonomy in order to accompany the fast-paced developments of AR technologies.

4.2. Enable and Foster Learning Processes about AR

The second approach acknowledges that, in the end, it is still the individual who makes the decision about whether to use a service or not. Thus, all technological solutions can only be seen as tools to support those who try to make deliberate and informed decisions related to their online privacy. However, findings in the literature on online privacy suggest that individuals who care about privacy and act upon it, for example, by spending money on privacy-enhancing technologies or by disclosing less or no personal data in social networks, represent the minority [49–51]. This is partly due to lack of interest, but also due to the complexity of privacy combined with time constraints, which yield to intuitive decisions related to privacy. Thus, many individuals rely on specific cues and heuristics to make privacy-related decisions in online environments [23]. Based on this, I argue that measures are needed to support individuals in these situations. It must be possible for individuals to learn about new information-processing practices that are applied by companies. In the past, individuals were able to learn about certain aspects of advertising on television over time and can now accurately recognize and most likely judge it as a way of influencing them [52,53]. However, this process of learning about influences over time might not always be possible for pervasive information technologies due to the aforementioned high levels of information asymmetry between companies and users. I would argue that the process of learning about the possibilities and threats of AR will take at least as much time as with comparable technological innovations like smartphones. However, there are three threats that can hinder this learning process.

First, the rapid technological developments in the field of AR can outrun individuals' ability to grasp them and make it difficult for them to derive practical recommendations for action in their daily lives. Second, there is always the risk that educational measures (e.g., in schools) only reach specific groups of people in society. Thus, regulating this educational aspect, e.g., by developing a "digital driver's license for AR", would be helpful in overcoming these problems and ensuring that people have the opportunity to learn about this technology if they wanted to. Third, certain practices of companies should undergo specific scrutiny. By now, it is common knowledge that individuals pay for free services with their data. Consequently, literature in the mobile app context shows that the price of an app affects users' privacy perceptions, as they tend to assume that free apps generate revenue by selling personal user data and paid apps by selling the app itself [54]. However, technical analyses show that both types of apps gather almost the same amount of personal data [55]. This scenario shows that the price cue would misguide an app user even if she or he would have knowledge about the use of personal data in exchange for free services.

4.3. Regulating Technological Developments before They Are Widely Used

This observation leads to the final approach of regulation. Regulatory interventions are required if the prior solutions do not achieve the desired effect, or if there are informational cues that were shown to mislead users in specific scenarios. I argue that we must consider the following aspects if autonomy serves as a guiding principle for evaluating possible regulations. First, it must be possible for individuals to have a choice in the first place. As discussed before, a loss of the ability to make decisions undermines the autonomy of individuals. There are examples from non-technical domains that show that individuals should be protected by regulatory authorities as soon as they are no longer able to decide about trade-offs (e.g., air pollution).

In the case of privacy-related decisions, individuals must be able to receive opt-in or opt-out options related to privacy-invasive practices. However, recent years showed an alarming development regarding the availability of these options. A new paradigm regarding the choice architecture about privacy-related decisions appears to gain traction. The paradigm is crisply summarized by the quote: "Bend the knee or we degrade your purchase" [11]. Such choice architectures deviate drastically from other "behavior-changing" concepts like the previously discussed concept of nudging, since the choice itself is either hidden or non-existent in the first place [26]. For example, iRobot, a manufacturer of robotic vacuum cleaners, announced selling floor plans of users in 2017 with an opt-out option [56]. However, the vacuum cleaner loses substantial connectivity features when users decide to protect their privacy and do not allow to share their floor plans (i.e., they opt out). This kind of choice architecture is equally problematic for the autonomy of individuals when they only have a skewed choice that appears as having freedom of choice about privacy that they actually do not have. Thus, there are choices that must be made possible by developers or that must be enforced in certain scenarios by regulators.

AR technologies use several sensitive permissions, which, alone, are perceived as critical by the study participants [31]. However, there is a second dimension that is not covered by the permission model, i.e., the combination of different pieces of information from different permissions, posing a much greater threat to privacy than the individual permission alone. Past research shows that a few pieces of information are usually enough to deanonymize individuals with a large probability [57]. There is no individual choice about the fact that companies combine such data in the current permission model. Thus, regulations of information provisioning in this context could help to provide transparency and fair choices. However, related work on privacy-enhancing technologies (PETs) and user acceptance indicates that, even given the opportunity, a majority of users will not use technologies to protect their privacy on the internet (especially if there is an explicit cost in the form of money or an implicit cost in form of time or higher effort involved with the use of PETs) [50,58–63]. Thus, we must rather think about combining the proposed measures from before with clear regulations on what AR technologies are allowed to do. This, in turn, can lead to a comprehensive approach to protect users' privacy and autonomy. Although there is always the threat that technological developments outrun regulatory interventions, I still argue that—given the timely input by expert practitioners and researchers—it is still possible to provide useful guidelines for privacy-friendly AR technologies.

5. Conclusions

To provide this input to practitioners and developers, a multidisciplinary research agenda is needed for addressing the pressing issues of privacy and security related to AR. First, the privacy risks associated with newest AR devices and their role within the context of the coming digital twins of the real world (such as the metaverse) must be analyzed based on technical analyses and expert interviews. For that purpose, our knowledge from prior work on existing AR technologies, such as mobile AR apps [31,48], can serve as a starting point to investigate newer types of AR technologies (e.g., AR wearables) for the consumer market.

These insights should be augmented with proposals for technical implementations of transparency-enhancing technologies (TETs), as I identified that transparency is a key principle for ensuring autonomy in the era of AR. These TETs must be especially designed with the importance of context in mind (see the discussion on contextual integrity [39]) and they need to consider how contextually relevant information can be shown to users while keeping usability aspects in mind. Such implementations must be evaluated with large-scale user studies to derive final technical, regulatory, and educational recommendations in order to foster privacy-friendly AR systems for the end-user market. These large-scale evaluations will be one of the key challenges researchers need to overcome when dealing with a technology like AR that is not widely diffused in the mass market yet. The future of augmented reality and all related concepts such as the metaverse will be decided in the coming months, and it is up to us whether privacy and human autonomy will be part of that future or not.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dejan, G. 29+ Augmented Reality Stats to Keep You Sharp in 2020. Available online: https://techjury.net/blog/augmented-reality-stats/ (accessed on 27 August 2020).
2. Petrock, V. US Virtual and Augmented Reality Users 2020. Available online: https://www.emarketer.com/content/us-virtual-and-augmented-reality-users-2020 (accessed on 27 August 2020).
3. Meta Introducing Meta: A Social Technology Company. Available online: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/ (accessed on 17 November 2021).
4. Levy, S. AR Is Where the Real Metaverse Is Going to Happen. Available online: https://www.wired.com/story/john-hanke-niantic-augmented-reality-real-metaverse/ (accessed on 17 November 2021).
5. Niantic Labs Official Website of Niantic Labs. Available online: https://www.nianticlabs.com/ (accessed on 3 May 2017).
6. Palladino, T. Niantic Opens Private Beta for AR Cloud Platform Now Called Lightship. Available online: https://next.reality.news/news/niantic-opens-private-beta-for-ar-cloud-platform-now-called-lightship-0384633/ (accessed on 17 November 2021).
7. Cook, T. Apple CEO Tim Cook Thinks Augmented Reality Will Be as Important as "Eating Three Meals a Day". Available online: http://www.businessinsider.com/apple-ceo-tim-cook-explains-augmented-reality-2016-10?r=US&IR=T (accessed on 27 January 2017).
8. Kaufmann, F.; Rook, L.; Lefter, I.; Brazier, F. *Understanding the Potential of Augmented Reality in Manufacturing Environments BT—Information Systems and Neuroscience*; Davis, F.D., Riedl, R., vom Brocke, J., Léger, P.-M., Randolph, A.B., Müller-Putz, G., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 128–138.
9. Baabdullah, A.M.; Alsulaimani, A.A.; Allamnakhrah, A.; Alalwan, A.A.; Dwivedi, Y.K.; Rana, N.P. Usage of Augmented Reality (AR) and Development of e-Learning Outcomes: An Empirical Evaluation of Students' e-Learning Experience. *Comput. Educ.* **2022**, *177*, 104383. [CrossRef]
10. Ho, V. Tech Monopoly? Facebook, Google and Amazon Face Increased Scrutiny. Available online: https://www.theguardian.com/technology/2019/jun/03/tech-monopoly-congress-increases-antitrust-scrutiny-on-facebook-google-amazon (accessed on 18 April 2020).
11. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; Profile Books; Public Affairs: New York, NY, USA, 2019.
12. Whitler, K.A. Why Too Much Data Is a Problem and How to Prevent It. Available online: https://www.forbes.com/sites/kimberlywhitler/2018/03/17/why-too-much-data-is-a-problem-and-how-to-prevent-it/#6b8632eb755f (accessed on 18 April 2020).
13. Chapple, C. Pokémon GO Has Best Year Ever in 2019, Catching Nearly $900 Million in Player Spending. Available online: https://sensortower.com/blog/pokemon-go-has-best-year-ever-in-2019-catching-nearly-900m-usd-in-player-spending (accessed on 3 April 2020).
14. D'Anastasio, C.; Mehrotra, D. The Creators of Pokémon go Mapped the World. Now They're Mapping You. Available online: https://kotaku.com/the-creators-of-pokemon-go-mapped-the-world-now-theyre-1838974714 (accessed on 2 April 2020).
15. Biddle, S. Privacy Scandal Haunts Pokemon Go's CEO. Available online: https://theintercept.com/2016/08/09/privacy-scandal-haunts-pokemon-gos-ceo/ (accessed on 20 April 2020).
16. Hanke, J. Guest Speaker Interview with John Hanke, CEO of Niantic, Inc. Available online: https://executive.berkeley.edu/thought-leadership/video/guest-speaker-interview-john-hanke-ceo-niantic-inc (accessed on 14 April 2020).

17. Thaler, R.H.; Sunstein, C.R. *Nudge: Improving Decisions about Health, Wealth, and Happiness*; Yale University Press: New Haven, CT, USA, 2008.
18. Sunstein, C. The Ethics of Nudging: An Overview. *Yale J. Regul.* **2015**, *32*, 413–450. [CrossRef]
19. Pichert, D.; Katsikopoulos, K.V. Green Defaults: Information Presentation and pro-Environmental Behavior. *J. Environ. Psychol.* **2008**, *28*, 63–73. [CrossRef]
20. Tversky, A.; Kahneman, D. Judgment under Uncertainty: Heuristics and Biases. *Science* **1974**, *185*, 1124–1131. [CrossRef]
21. Thaler, R.H. Mental Accounting and Consumer Choice. *Mark. Sci.* **2008**, *27*, 15–25. [CrossRef]
22. Kahneman, D. *Thinking, Fast and Slow*; Farrar, Straus and Giroux: New York, NY, USA, 2011.
23. Dinev, T.; Mcconnell, A.R.; Smith, H.J. Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Inf. Syst. Res.* **2015**, *26*, 639–655. [CrossRef]
24. Schubert, C. *On the Ethics of Public Nudging: Autonomy and Agency*; MAGKS Papers on Economics; Philipps-Universität Marburg, Faculty of Business Administration and Economics, Department of Economics: Marburg, Germany, 2015; pp. 1–26.
25. van den Hoven, M. Nudging for Others' Sake: An Ethical Analysis of the Legitimacy of Nudging Healthcare Workers to Accept Influenza Immunization. *Bioethics* **2020**, *35*, 143–150. [CrossRef]
26. Susser, D.; Roessler, B.; Nissenbaum, H. Technology, Autonomy, and Manipulation. *Internet Policy Rev.* **2019**, *8*, 1–22. [CrossRef]
27. Thaler, R. The Power of Nudges, for Good and Bad. Available online: https://www.nytimes.com/2015/11/01/upshot/the-power-of-nudges-for-good-and-bad.html (accessed on 17 December 2020).
28. Sanchez-Rola, I.; Dell'Amico, M.; Kotzias, P.; Balzarotti, D.; Bilge, L.; Vervier, P.-A.; Santos, I. Can i Opt out yet? Gdpr and the Global Illusion of Cookie Control. In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Auckland, New Zealand, 9–12 July 2019; pp. 340–351.
29. Rauschnabel, P.A.; He, J.; Ro, Y.K. Antecedents to the Adoption of Augmented Reality Smart Glasses: A Closer Look at Privacy Risks. *J. Bus. Res.* **2018**, *92*, 374–384. [CrossRef]
30. Harborth, D.; Pape, S. Investigating Privacy Concerns Related to Mobile Augmented Reality Applications. In Proceedings of the International Conference on Information Systems (ICIS), Munich, Germany, 15–18 December 2019; pp. 1–9.
31. Harborth, D.; Pape, S. Investigating Privacy Concerns Related to Mobile Augmented Reality Applications—A Vignette Based Online Experiment. *Comput. Hum. Behav.* **2021**, *122*, 106833. [CrossRef]
32. Harborth, D.; Kreuz, H. Exploring the Attitude Formation Process of Individuals Towards New Technologies: The Case of Augmented Reality. *Int. J. Technol. Mark.* **2020**, *14*, 125–153. [CrossRef]
33. Harborth, D. Unfolding Concerns about Augmented Reality Technologies: A Qualitative Analysis of User Perceptions. In Proceedings of the Wirtschaftsinformatik (WI19), Siegen, Germany, 24–27 February 2019; pp. 1262–1276.
34. Harborth, D.; Hatamian, M.; Tesfay, W.B.; Rannenberg, K. A Two-Pillar Approach to Analyze the Privacy Policies and Resource Access Behaviors of Mobile Augmented Reality Applications. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019; pp. 5029–5038.
35. Denning, T.; Dehlawi, Z.; Kohno, T. In Situ with Bystanders of Augmented Reality Glasses. In Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems—CHI '14, Toronto, ON, Canada, 26 April–21 May 2014; pp. 2377–2386.
36. Lebeck, K.; Ruth, K.; Kohno, T.; Roesner, F. Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users. In Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 21–23 May 2018; pp. 392–408.
37. de Guzman, J.A.; Thilakarathna, K.; Seneviratne, A. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *arXiv* **2018**, arXiv:1802.05797v2. [CrossRef]
38. European Union. Charter of Fundamental Rights of the European Union. Available online: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed on 20 May 2022).
39. Nissenbaum, H. *Privacy in Context: Technology, Policy and the Integrity of Social Life*; Stanford University Press: Palo Alto, CA, USA, 2010.
40. Nissenbaum, H. Contextual Integrity Up and Down the Data Food Chain. *Theor. Inq.* **2019**, *20*, 221–256. [CrossRef]
41. Herzog, L. Citizens' Autonomy and Corporate Cultural Power. *J. Soc. Philos.* **2020**, *51*, 205–230. [CrossRef]
42. Christman, J. Autonomy in Moral and Political Philosophy. Available online: https://plato.stanford.edu/entries/autonomy-moral/ (accessed on 1 May 2022).
43. Dworkin, G. *The Theory and Practice of Autonomy*; Cambridge University Press: New York, NY, USA, 1988.
44. Beauchamp, T.L.; Childress, J.F. *Principles of Biomedical Ethics*; Oxford University Press: Oxford, UK, 2013.
45. Halper, T. Privacy and Autonomy: From Warren and Brandeis to Roe and Cruzan. *J. Med. Philos.* **1996**, *21*, 121–135. [CrossRef]
46. Jacobs, N. Two Ethical Concerns about the Use of Persuasive Technology for Vulnerable People. *Bioethics* **2020**, *34*, 519–526. [CrossRef]
47. McDonald, A.M.; Cranor, L.F. The Cost of Reading Privacy Policies. *I/S A J. Law Policy Inf. Soc.* **2008**, *4*, 543.
48. Harborth, D.; Frik, A. Evaluating and Redefining Smartphone Permissions for Mobile Augmented Reality Apps. In Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS 2021), Virtual, 8–10 August 2021; pp. 513–533.
49. Spiekermann, S.; Grossklags, J.; Berendt, B. E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. In Proceedings of the Third ACM Conference on Electronic Commerce, Seoul, Korea, 3–5 August 2015; ACM: Tampa, FL, USA, 2001; pp. 38–47.

50. Grossklags, J.; Acquisti, A. When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In Proceedings of the WEIS, Hanover, NH, USA, 25–27 June 2007.
51. Harborth, D.; Cai, X.; Pape, S. Why Do People Pay for Privacy-Enhancing Technologies? The Case of Tor and JonDonym. In Proceedings of the ICT Systems Security and Privacy Protection, SEC 2019, Lisbon, Portugal, 25–27 June 2019; IFIP Advances in Information and Communication Technology; Dhillon, G., Karlsson, F., Hedström, K., Zúquete, A., Eds.; Springer: Cham, Switzerland, 2019; Volume 562, pp. 253–267.
52. Seels, B.; Fullerton, K.; Berry, L.; Horn, L.J. Research on Learning from Television. In *Handbook of Research on Educational Communications and Technology*, 2nd ed.; Hardcover; Lawrence Erlbaum Associates Publishers: Mahwah, NJ, USA, 2004; pp. 249–334, ISBN 0-8058-4145-8.
53. Olney, T.J.; Holbrook, M.B.; Batra, R. Consumer Responses to Advertising: The Effects of Ad Content, Emotions, and Attitude toward the Ad on Viewing Time. *J. Consum. Res.* **1991**, *17*, 440–453. [CrossRef]
54. Bamberger, K.A.; Egelman, S.; Han, C.; Elazari, A.; On, B.; Reyes, I. Can you pay for privacy? Consumer expectations and the behavior of free and paid apps. *Berkeley Technol. Law J.* **2020**, *35*, 1174616.
55. Han, C.; Reyes, I.; Elazari, A.; On, B.; Reardon, J.; Feal, Á.; Bamberger, K.A.; Egelman, S.; Vallina-rodriguez, N. Do You Get What You Pay For? Comparing the Privacy Behaviors of Free vs. Paid Apps. In Proceedings of the Workshop on Technology and Consumer Protection (ConPro '19), San Francisco, CA, USA, 23 May 2019; pp. 1–7.
56. O'Neill, N. Roomba Maker Wants to Sell Your Home's Floor Plan. Available online: https://nypost.com/2017/07/25/roomba-maker-wants-to-sell-your-homes-floor-plan/ (accessed on 20 April 2020).
57. de Montjoye, Y.-A.; Radaelli, L.; Singh, V.K.; Pentland, A. Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata. *Science* **2015**, *347*, 536–539. [CrossRef]
58. Harborth, D.; Pape, S. Examining Technology Use Factors of Privacy-Enhancing Technologies: The Role of Perceived Anonymity and Trust. In Proceedings of the 24th Americas Conference on Information Systems, New Orleans, LA, USA, 16–18 August 2018.
59. Harborth, D.; Herrmann, D.; Köpsell, S.; Pape, S.; Roth, C.; Federrath, H.; Kesdogan, D.; Rannenberg, K. Integrating Privacy-Enhancing Technologies into the Internet Infrastructure. *arXiv* **2017**, arXiv:1711.07220.
60. Harborth, D.; Pape, S. JonDonym Users' Information Privacy Concerns. In Proceedings of the ICT Systems Security and Privacy Protection, SEC 2018, Poznan, Poland, 18–20 September 2018; IFIP Advances in Information and Communication Technology; Janczewski, L., Kutyłowski, M., Eds.; Springer: Cham, Switzerland, 2018; Volume 529, pp. 170–184.
61. Harborth, D.; Pape, S.; Rannenberg, K. Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. *Proc. Priv. Enhanc. Technol.* **2020**, *2020*, 111–128. [CrossRef]
62. Harborth, D.; Pape, S. How Privacy Concerns, Trust and Risk Beliefs, and Privacy Literacy Influence Users' Intentions to Use Privacy-Enhancing Technologies: The Case of Tor. *ACM SIGMIS Database Adv. Inf. Syst.* **2020**, *51*, 51–69. [CrossRef]
63. Harborth, D.; Pape, S. How Privacy Concerns and Trust and Risk Beliefs Influence Users' Intentions to Use Privacy-Enhancing Technologies—The Case of Tor. In Proceedings of the Hawaii International Conference on System Sciences (HICSS) Proceedings, Maui, HI, USA, 8–11 January 2019; pp. 4851–4860.