Informed Digital Consent for Use of AI Systems Grounded in a Model of Sexual Consent

Emmie Hine

{emmie.e.hine@gmail.com}

Oxford Internet Institute, University of Oxford, U.K.

Abstract. Artificial intelligence (AI) systems shape our infospheres, mediating our interactions and defining what information we have access to. This poses a tremendous threat to individual autonomy and impacts society, both online and offline. Users are often unaware of the potential impacts of using these systems, and companies that utilise them are not incentivised to adequately inform their users of those impacts. Forms of digital design ethics, including pro-ethical design and tolerant paternalism, have been proposed to help protect user autonomy, but are not sufficient to ensure that users are educated enough to make informed decisions. In this paper, I use sexual consent as defined by American universities to outline and propose ways to implement a model of "informed digital consent" that would ensure that users are well-informed so that their autonomy is not only respected, but enhanced.

Keywords: Consent, artificial intelligence, tolerant paternalism, infosphere, autonomy

1 Introduction

One major ethical concern about the rise of artificial intelligence (AI) systems in society is the challenge to human agency and autonomy that they present. Like Taddeo and Floridi state, "As it matures and disseminates, AI blends into our lives, experiences, and environments and becomes an invisible facilitator that mediates our interactions in a convenient, barely noticeable way" [1]. In other words, AI becomes thoroughly integrated and normalised in our lives, which results in its impacts being overlooked. This "invisible AI" could threaten our "ability to determine our own lives and identities and keep our choices open" [1]. When it comes to something like a music recommendation system, this threat to autonomy may seem overblown. However, when these algorithms define the information users have access to—like Facebook's News Feed algorithm or Google search rankings—it becomes more crucial to ensure that users are informed and able to judge for themselves the acceptable impact of these algorithms. In this paper, I will be addressing AI systems that define and shape individuals' interactions with the infosphere. The term "infosphere" minimally "denotes the whole informational environment constituted by all informational entities (thus including information agents as well), their properties, interactions, processes, and mutual relations" [2]. In other words, it constitutes a realm of information and data, but is not solely limited to online spaces. AI algorithms that mediate individuals' interactions with the infosphere include recommender

CAIP 2021, November 20-24, Bologna, Italy

DOI 10.4108/eai.20-11-2021.2314136

systems, such as those used by Netflix and Spotify, but also broader-scope algorithms, like the aforementioned Facebook News Feed algorithm and advertisement targeting algorithms. I argue that in order to ensure that user autonomy is respected by corporate AI systems, we must augment current design models with a consent system inspired by sexual consent as defined by American universities.

It should be noted that the threats posed by AI go beyond just user agency and autonomy; the preservation of both is necessary but not sufficient for an AI system to be ethical. The EU guidelines for ethical AI, which are designed to support human autonomy, include the principles of:

- Human agency and oversight
- Robustness and safety
- Privacy and data governance
- Transparency
- Diversity, nondiscrimination and fairness
- Societal and environmental well-being
- Accountability [3]

Some level of threat to human agency is inherent to many AI systems. However, with systems that shape the infosphere, the threat is larger and has knock-on effects to broader society. For instance, echo chambers and filter bubbles created by infosphere-shaping algorithms entrench polarisation and disinformation. This has broader impacts, including motivating many rioters in the January 6 attack on the US Capitol [4]. By impacting their beliefs about election fraud, AI systems shaped individual interactions with the infosphere, which together had an enormous impact on society, online and offline. In order to foster agency, transparency, and accountability, users must be aware of the potential consequences of using the systems, which can include impacts on their own person and society as a whole. Thus, adequate user consent is necessary for the ethical use of these systems—what I define as "informed digital consent."

2 Digital design ethics

When it comes to digital design ethics, there are several approaches. The first is "ethics by design," which embeds ethical values into technology design from the very beginning of the process. Ethics by design enforces certain ethical values by designing to make certain actions easier or more difficult. "Structural nudging" is an approach that "seeks to shape agents' environments and their available course of action" by providing alternative options. The more successful these approaches are, the more they in fact violate user autonomy, as they shape agents' behaviour and disempower them to make their own choices by pushing users towards predefined actions [5]. In addition, these option-shaping approaches require great trust in whoever is deciding what values to endorse in a system's design. They actually allow for the subversion of consent, as in the case of an opt-out organ donation system, which is unacceptable when looking at systems that could have significant impact on users.

"Pro-ethical design," on the other hand, works to help users "empower themselves" by making choices based on the information provided. One form is "informational nudging," which gives them information about the options available to them. Another form is "mandated choice," which places a choice that an agent has to make between the agent and an action, like making a driver choose whether or not to become an organ donor when renewing their licence. This is a kind of "tolerant paternalism;" the design is paternalistic by forcing the user to make a choice, but tolerant because it enables and permits different behaviours [5]. So, for a user consent system, tolerant paternalism makes the user choose whether or not to give consent. While this model does a good job of empowering users and respecting user autonomy in situations where the level of information required is relatively low, it contains no requirements to ensure that users are adequately informed in situations where a higher level of knowledge or understanding is required.

3 The failure of tolerant paternalism to inform

Tolerant paternalism places user autonomy at its core, but inherently contains an acknowledged "tension between mandate choice and informed consent." Tolerant paternalism forces agents to make a choice, but it does not require that that choice be informed. Rather, it focuses on making users "acknowledge the presence of a question and to answer it" with a "personal choice" [5]. If the choice is a relatively complex one, though, then by not ensuring that the agent is appropriately informed to make the choice, we are not being sufficiently paternalistic. Furthermore, if this choice is presented at a time when the user is impatient to get to whatever is beyond the choice—such as an online service—the user may not thoroughly consider the ramifications of their choice. We cannot claim that we are enhancing an agent's autonomy when we are not providing them with the resources needed to make the choice that is best for them.

4 A sexual consent model for digital consent

In many American universities, sexual consent is taught as an affirmative "yes-means-yes" policy. California and the State University of New York system have adopted a definition of sexual consent as "an affirmative, unambiguous, and conscious decision by each participant to engage in mutually agreed-on sexual activity;" more than 800 individual universities have adopted similar definitions [6]. Though affirmative consent policies differ in wording across the country, they all include a requirement for "freely expressed willingness" and "active participation from all parties" for a specific activity [7]. For the purposes of this paper, the key components of consent are the requirements that the action is only taken if the consent is affirmative; that all parties be adequately informed; that consent is a continuous, evolving dialogue between parties; and that parties are able to withdraw consent at any time. Derived from the requirement for adequate information, I will argue that each participant has a positive duty to prevent harm to all other parties. In the remainder of this paper, I explore how these requirements can apply to AI systems to ensure that user autonomy is protected, then discuss possible implementation measures for a model of "informed digital consent."

The first requirement is that consent be affirmative. This means that it must be both positive and not coerced. Tolerant paternalism requires that agents be given equal opportunity to choose "yes" or "no" when making their choice. Models which require that users consent to the use of AI in order to access a service violate this principle, as unless AI is integral to the service, a company would merely prefer that users accept its use because it aids their profit. The consent must also be unambiguously affirmative; technology consent is always a yes-or-no choice, removing ambiguity. The possibility that a user be unsure and select "yes" anyways is prevented by the adequate information requirement, which I will discuss next.

Second, in order for consent to be valid under this model, it must be conscious and adequately informed. Just as sexual consent cannot be given when one party is too intoxicated or otherwise impaired to understand what they are consenting to, consent should not be valid when a user does not truly understand what they are consenting to by accepting the use of an AI system. Thus, agreements cannot be like the cookie consent banners seen on many websites that often require effort to find the "deny cookies" option. These pop-ups are designed to be "consented" to and clicked away as quickly as possible, which is unacceptable under the sexual consent model. Users cannot be badgered into giving consent; AI system consent tools must be designed to engage the user instead of encouraging them to give in as quickly as possible. There is precedent for these requirements in data privacy law. The GDPR states that declarations of consent provided to users must be "intelligible and easily accessible" and that "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment" [8]. Furthermore, special care must be taken when there are significant power imbalances between the user and data controller [9], which is mirrored in the relationship between users and large platforms. This vests significant responsibility on the platforms. The requirement to ensure that users are adequately informed will necessitate effort on the part of platforms to ensure that users are appropriately educated about the potential effects of AI systems, which may be difficult for the average user to predict due to the complex nature of such systems. In order to be "tolerant" and respect user autonomy, we must allow them to make choices that may result in their autonomy being infringed upon by AI systems, but to be adequately "paternalistic," they must prove that they understand the ramifications of this choice. One possible form this could take is a short educational module; I will discuss implementation details further in the next section, but this is a significant responsibility that will require cooperation between platforms, governments, and third-party organisations to ensure that education is adequate and accessible for all users. This would also create a significant regulatory burden, the ramifications of which will be discussed later.

Third, consent must be dynamic and evolving, a two-way conversation between platforms using AI systems and its users. As platforms and their AI systems evolve, users must be kept aware of how the systems are changing and how those changes may impact them. In the sexual consent model, agents give consent for a specific activity, so if that activity changes, consent must be obtained for the new activity. There are technical precedents for this in the "Dynamic Consent" project, an architecture developed for biomedical research. The Dynamic Consent model "is an approach to consent that enables people, through an interactive digital interface, to make granular decisions about their ongoing participation" [10, 11]. Participants have access to a user-friendly interface that enables users to easily alter their consent choices and, crucially, to engage with researchers. This enables users to ask questions

about projects, serving as an informational source that empowers users to give or withhold truly informed consent [10]. Though Facebook and other platforms have created privacy centres and checkup tools, these are at best superficial aids and at worst deliberately hidden but highly touted ethics-washing[1] tools. They focus on privacy and data protection and contain no information about the AI systems that may be impacting user autonomy. Users need effective interfaces and actual communication from platforms to decide what level of interaction with AI systems they are comfortable with, as such systems could have substantial impacts on their individual well-being—both from their own actions and those of others—and knock-on effects to the rest of society. These "invisible" effects threaten self-determination in ways that could range from purchasing something a user otherwise would not have to real-world violence [1], as seen in the Capitol riots. An awareness of how damage to the infosphere damages all of us can create both selfish and altruistic assumption of individual responsibility online.

Taken in aggregate, these responsibilities imply a positive moral duty on all parties involved to ensure that other parties are not unknowingly being subject to harm.[2] Under the sexual consent model, agents consent to a specific activity with reasonably foreseen consequences. If unforeseen or excessively negative consequences arise and if other agents involved are aware of those consequences, they have a moral obligation to make the impacted agent aware. Regarding AI systems, users may be educated on the possible impacts of an AI system and consent, but if the real impacts of the system are beyond what could have reasonably been predicted, the platform has a duty to make them aware and rectify those impacts. For example, in the event that a platform detects that a user is falling into a "filter bubble" and becoming more polarised, it should alert the user, invite them to revisit their consent, and then take measures to prevent anti-social outcomes. It should do this even if a user has been informed that polarisation is a possible side effect of using a platform, as consenting to use a service that poses a risk of negative impacts does not imply consent to those negative effects. Each party's duties to the others and the trust inherent to a relationship of affirmative consent means that there is a duty of protection. This may be a way to mitigate the anti-social outcomes that AI systems can foster without requiring a wholesale alteration of platform AI systems.

5 Implementation of informed digital consent

While a model of what I call "informed digital consent" seems appealing in that it would protect individuals from harm perpetuated by AI systems and prevent anti-social outcomes (including but not limited to the aforementioned increase in polarisation and the associated knock-on effects), implementation of this model would be difficult in practice. We must ensure that all users of services that incorporate infosphere-shaping AI algorithms are sufficiently educated about their effects and have a meaningful understanding of what

[1] Ethics-washing is the practice of "fabricating or exaggerating" a company's perceived commitment to ethical behaviour and is harmful because it distracts from the need for real, effective measures [12].

[2] As sexual consent is a two-way model, this also implies that users have equivalent duties to not harm the platforms. Due to the power dynamics of the user-platform relationship, however, it is difficult to imagine what damage a user could do to a platform in this arrangement, with the exception of hacking or other manipulation, which would already be prohibited by the law and a platform's terms of service.

consenting to use the service entails. As previously mentioned, this could take the form of short educational modules on the various systems in use. However, the scope of this effort will be unprecedented. Facebook alone had 2.7 billion monthly active users as of the second quarter of 2020, and Google, which dominates the targeted advertising business with an 86% search engine worldwide market share, is almost synonymous with the Internet [13, 14]. As a result of the global reach of the Internet, users vary in terms of language, geography, education level, cultural background, and almost any other conceivable factor. Thus, no single education module will work for every user. To overcome this hurdle, we can again look towards sexual consent as taught in American universities.

In America, Title IX of the Education Amendments of 1972 prohibits sex-based discrimination in universities that receive federal funding, which is nearly all universities[15]. Since 2011, sexual harassment and violence has been interpreted as a form of sex discrimination under Title IX, requiring universities to "take immediate and effective steps to end sexual harassment and sexual violence" [16]. As part of these efforts, many universities try to educate students on affirmative consent.

This often takes the form of educational seminars on consent at the start of the year, often during orientation days for first-year students. Schools sometimes bring in outside groups, such as Speak About It, which "uses theater and dialogue to empower students to give and get consent, build healthy relationships, and make change in their communities" [17]. These groups liaise with on-campus peer leaders and peer educators to facilitate discussion and ensure that all students have a common grounding in affirmative consent [18]. Because they are outside organisations, they have no conflicts of interest, and are able to approach students from a more accessible perspective than that of a school administration. So, entrusting this education to an outside group, albeit one that liaises with platforms to ensure that they have a comprehensive understanding of the issues at play, is an important component of effective consent education.

To ensure consistent quality of education and avoid the fragmentation seen across universities, all education done in the name of informed digital consent should be centralised under a single body. This could be a federal entity, or it could be an organisation funded by platforms but that operates independently. The benefit of a group focused solely on consent education is that because they specialise in the topic, these groups acknowledge that consent education is not a one-size-fits-all endeavour; different schools have different cultures, and groups within the same university (e.g., athletes versus non-athletes) may require different approaches. Similarly, different user groups will require different approaches to ensure informed digital consent. This is where the sheer quantity of data that platforms have on users can be useful; platforms can use methods based on big data to match users to an education program in their language tailored to their education level and familiarity with technology. New users could provide a limited amount of information to match them to a program; this data should not be retained for the platform's use.

The idea of mandating educational modules before a user can access a platform that uses infosphere-mediating AI may seem like ridiculous regulatory overreach, but responsible engagement with these platforms is a new type of civic duty. According to Oxford historian Dr. Joanna Innes, the core of the idea of a civic duty is the need to preserve the public good [19]. Thus, civic duties bestow a responsibility on the individual to behave in a way that

upholds societal order, and are often legislated or otherwise encouraged by the state. In other words, individuals have a responsibility to inform themselves on how to behave "well" and protect society, and platforms have a responsibility to facilitate that. As seen in the Capitol riots, engagement with infosphere-shaping systems can result in major negative impacts to social order, meaning we have a responsibility to engage with them responsibly. Similarly, because of the impact violations of consent have on the health and safety of a society, practicing affirmative sexual consent should be considered a civic duty, but often is not—only eight states require sex education classes to mention consent, and they do not say anything about what model of consent should be taught [20].

Other civic duties are treated with more seriousness by legislators; for example, responsible driving. One's actions on the road—especially how they coordinate with other drivers in the road system—impact the safety of society. Driving responsibly is a civic duty; to educate people on how to do so, driver's education is mandatory for teenage drivers in 32 states, and all new drivers must pass a road driving test [21, 22]. Part of a driver's education course is teaching drivers about the possible ramifications of driving; the California Highway Patrol produced a series called "Red Asphalt," a gory display of real road accidents described as "driver's-ed snuff movies" and shown across the country [23]. Drivers are taught about the possible negative impacts of driving and how to avoid them. Similarly, consent education teaches about the deleterious effects of violating affirmative consent and teaches students how to protect themselves and avoid harming others. As civic duties, both involve education to ensure proper behaviour and protect society. As discussed previously, AI systems can infringe on user autonomy and negatively affect individuals and, by extension, others in the community and the community as a whole. Informed digital consent education should educate users on how interacting with infosphere-mediating AI systems can impact them and in turn how those actions can impact others and society as a whole.

Even though the rules of the road rarely change, many states require drivers to re-take the driving test every so often (especially older drivers) and affirmative consent rules are often re-hashed even for upperclassmen at the beginning of the school year. If even more or less static civic duties require periodic re-education, anything dealing with the ever-changing Internet will require frequent refreshers. It seems reasonable that any time a major update to an AI service is performed, users should be taught about how it may impact them so that they can, in the style of Dynamic Consent, re-evaluate whether they want to continue to use the platform. How often to do so, however, will depend on the platform, AI service, and impact of updates. For example, Google updates its search ranking algorithm frequently, sometimes multiple times per month [24]. Requiring an entire education model for every small algorithmic tweak would be unduly burdensome; explaining a fix that repairs "the bulk of indexing and canonicalization bug(s)" would be unnecessary and overly burdensome for educators and users [24]. Thus, the frequency of refreshers should be predicated on the level of risk an AI service poses. Spotify should not have to re-educate its users about its music recommendation algorithm as often as, say, Facebook should have to about its targeted advertisement algorithm.

A baseline of annual refreshers seems reasonable, with their content and duration dependent on the complexity and risk of the services, and the opportunity to withdraw consent and cease using the AI service provided. It may also be helpful to deploy smaller refreshers or informational notifications during elections or major public disaster when misinformation is

likely to spread. There is already precedent for this with Facebook's efforts to combat COVID-19 misinformation by directly notifying users who like or share posts later removed for violating the terms of service that they were exposed to misinformation; users are also prompted with informational links and actions like unfollowing the entity that shared the post [25]. In addition, since consent must be a dynamic conversation, enabling users to inquire about AI systems could help protect them and possibly reduce the required frequency of full refreshers. As discussed above, when a service changes significantly, users should be informed of the changes and offered the same opportunity to withdraw consent. Finally, if the platform detects that a user is being harmed by its services, the platform is obliged to stage an intervention. This is another instance where a platform's vast quantity of information can come in handy; interventions can be targeted based on user characteristic and the type of harm.

6 Addressing violations of informed digital consent

Interventions are obligatory between partners when something someone has consented to has unforeseen or unduly negative consequences. In that situation, so long as the intervention occurs, no one is at fault. However, what is to be done when consent is deliberately violated? On American campuses, cases of sexual harassment—defined as including "sexual assault, dating violence, domestic violence, and stalking"—can be handled both by the school's disciplinary process and by the legal system [26]. Violation of digital consent could entail forcing or coercing a user into an activity or service that they did not expressly consent to. To review, the four components of consent we are considering are that it be affirmative, conscious and informed, and a dynamic conversation, as well as the duty to prevent harm. A violation could entail subjecting a user to a service they were not informed about, which would violate the affirmative consent requirement. It could also involve duping users into consenting to a service by misrepresenting or omitting information about it, which would violate the adequate-information principle of informed consent, or a platform making significant changes to a service and not informing users about it, which would violate the continuous "conversation" principle. Finally, it could involve a platform becoming aware that users are being unduly harmed by a service and not fulfilling its obligation to inform them.

Violation of the principles of informed digital consent could be handled either by the legal system or an external body. For cases to be handled by the legal system, definitions of informed legal consent would have to be enshrined in law with clear sanctions and enforcement mechanisms, as well as a redefinition of what constitutes a crime against platform users. Because of different definitions of consent, not every action that violates a campus sexual assault regulation is considered a crime by the judicial system; this kind of fragmentation is unacceptable. The American legal system (with the exception of California) has yet to be able to cohesively define affirmative sexual consent, much less how—or even if—consent education should be mandated. Even for topics more traditionally acknowledged as civic responsibilities, like driving, different states have varying educational standards, and this does not even begin to address the varying standards worldwide. Because of the global scope of platforms that use infosphere-mediating AI systems, any regulation would also have to be global in scope and legislate what constitutes a violation of self-determination and autonomy in a culturally pluralistic way. Thus, it seems extremely unlikely that we would be

able to globally define affirmative digital consent or outline the kind of user education that would have to be undertaken to protect users.

Thus, an external body may be a better choice. This could be a group internal to a platform, but due to the inherent conflicts of interest that would create and potential fragmentations between platforms, would better be an external group. This could be the same group entrusted with educational efforts. The same group helping create educational modules with platforms would likely be best informed about the standards underlying their educational efforts, as well as what constitutes a violation to user autonomy and self-determination, and thus could help enforce the standards. This would require this group to be vested with significant power to sanction or fine violating platforms, perhaps requiring coordination with the UN, WHO, or a coalition of platforms; it could also utilise the framework of the International Organisation for Standardisation (ISO), which works with 165 countries to set international standards [27].

7 Conclusion

The idea of mandated choice in tolerant paternalism is valuable for the ethical use of autonomy-impacting AI systems because it requires user consent to proceed, respecting user autonomy by allowing them to choose to potentially sacrifice some agency. However, it must be augmented to require informed consent. Existing ethical design principles do not require an adequately informed consent decision and thus do not adequately protect user autonomy. When seeking consent for use of these systems, we should take inspiration from sexual consent as defined by American universities, which seeks to preserve individual autonomy in a system dubbed "informed digital consent." Thus, platforms seeking to use such tools must gain affirmative, educated, continuous consent from users, and must also protect users from otherwise unforeseen harms.

In this paper, I move beyond just design ethics to a specific model of digital consent, finding that for some AI-enabled digital systems, existing models of design ethics are inadequate to preserve user autonomy. AI ethics guidelines *imply* that adequate consent is necessary for ethical use of AI, but a new consent requirement could be explicitly incorporated into ethics frameworks and then into design frameworks. Because companies are more likely to embrace ethical design principles than frameworks that specifically govern the use of AI to preserve their bottom lines, explicitly outlining different models of consent and when they should be used may be a valuable exercise [12]. Overall, though, this form of consent requires an unprecedented level of transparency from platforms and a willing investment in user education. Especially for the informed consent requirement, there must be significant investment from private corporations, ideally in coordination with the public sector, to educate users and develop metrics to ensure that consent is adequately informed.

As I have shown, the implementation of informed digital consent will likely require the creation of an independent body, funded by the public sector and/or platforms that use potentially autonomy-impacting AI systems, similar to Facebook's Oversight Board. This body would be entrusted with devising a definition of informed digital consent, operationalising it through educational modules, and levying fines or other sanctions on platforms in violation. This would require a massive voluntary effort on the part of platforms

that use potentially autonomy-violating AI systems, possibly driven by users insisting that their autonomy be respected. While some users may disagree with the efforts, increasing user awareness of the impacts of these systems on our shared infosphere will push platforms to adopt to these standards. Incentivising this action may be where the legal system becomes useful, rather than in enforcing these standards. If voluntary action on the part of platforms is not forthcoming, laws could mandate that platforms fund the creation of this independent body and subject themselves to its rulings. This is likely to be a difficult task, but achievable. Like the GDPR required websites to ask user consent for cookie use (flawed though it is), and like the definition of sexual consent is codified in California law and many universities across America, we could regulate to ensure that platforms deploying AI systems will not infringe on user autonomy. Instead, platforms could actually enhance user autonomy by ensuring they are educated about the impacts of the systems that they interact with every day.

References

[1] Taddeo M, Floridi L. How AI can be a force for good | Science. *Science* 2018; 361: 751–752.

[2] Floridi L. *The Ethics of Information*. Oxford University Press, 2013.

[3] Madiega T. EU guidelines on ethics in artificial intelligence: Context and implementation. 13.

[4] Manser A. Impact on democracy, https://www.udel.edu/udaily/2021/january/capitol-attack-democracy-panel-discussion/ (2021, accessed 7 April 2021).

[5] Floridi L. Tolerant Paternalism: Pro-ethical Design as a Resolution of the Dilemma of Toleration. *Sci Eng Ethics*; 22. Epub ahead of print 1 December 2016. DOI: 10.1007/s11948-015-9733-2.

[6] New J. Colleges across country adopting affirmative consent sexual assault policies, https://www.insidehighered.com/news/2014/10/17/colleges-across-country-adopting-affirmative-consent-sexual-assault-policies (2014, accessed 24 February 2021).

[7] Harvard Political Review. Defining Affirmative Consent. *Harvard Political Review*, https://harvardpolitics.com/defining-affirmative-consent/ (2014, accessed 24 February 2021).

[8] Recital 42 - Burden of Proof and Requirements for Consent. *General Data Protection Regulation (GDPR)*, https://gdpr-info.eu/recitals/no-42/ (accessed 12 November 2021).

[9] Recital 43 - Freely Given Consent. *General Data Protection Regulation (GDPR)*, https://gdpr-info.eu/recitals/no-43/ (accessed 12 November 2021).

[10] Kaye J, Whitley EA, Lund D, et al. Dynamic consent: a patient interface for twenty-first century research networks. *Eur J Hum Genet* 2015; 23: 141–146.

[11] Prictor M, Lewis MA, Newson AJ, et al. Dynamic Consent: An Evaluation and Reporting Framework. *J Empir Res Hum Res Ethics JERHRE* 2020; 15: 175–186.

[12] Johnson K. How AI companies can avoid ethics washing. *VentureBeat*, https://venturebeat.com/2019/07/17/how-ai-companies-can-avoid-ethics-washing/ (2019, accessed 24 April 2021).

[13] Tankovska H. Facebook MAU worldwide 2020. *Statista*, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (2021, accessed 7 April 2021).

[14] Johnson J. Topic: Google. *Statista*, https://www.statista.com/topics/1001/google/ (2021, accessed 7 April 2021).

[15] Vedder R. There Are Really Almost No Truly Private Universities. *Forbes*, https://www.forbes.com/sites/richardvedder/2018/04/08/there-are-really-almost-no-truly-private-universities/ (2018, accessed 7 April 2021).

[16] Ali R. Dear Colleague Letter, https://www2.ed.gov/about/offices/list/ocr/letters/colleague-201104.html (2011, accessed 7 April 2021).

[17] Speak About It: Consent Education. *Speak About It: Consent Education*, https://wespeakaboutit.org (2021, accessed 7 April 2021).

[18] Flagship Show. *Speak About It: Consent Education*, https://wespeakaboutit.org/flagship-show (2021, accessed 7 April 2021).

[19] King V. Is there such a thing as civic duty? And do we feel it? *BBC News*, 24 November 2011, https://www.bbc.com/news/uk-politics-15763388 (24 November 2011, accessed 11 April 2021).

[20] Maxouris C, Ahmed S. Only these 8 states require sex education classes to mention consent. *CNN*, https://www.cnn.com/2018/09/29/health/sex-education-consent-in-public-schools-trnd/index.html (accessed 6 April 2021).

[21] DriversEd.com. Preparing to Become a New Driver: Which States Require Drivers Ed? *DriversEd.com*, https://driversed.com/trending/which-states-require-drivers-ed (2020, accessed 7 April 2021).

[22] Zakhareuski A. DMV Driving Test: Your Complete Guide to the Road Test. *Driving-Tests.org*, https://driving-tests.org/road-test/ (2020, accessed 7 April 2021).

[23] Smith MJ. The Peculiar Genius of the 'Red Asphalt' Road-Splatter Films. *Medium*, https://medium.com/@martinjsmith/the-cinematic-genius-of-the-red-asphalt-road-splatter-series-5289d382ffa3 (2017, accessed 7 April 2021).

[24] Google Algorithm Update History. *Moz*, https://moz.com/google-algorithm-change (2021, accessed 6 April 2021).

[25] Campbell IC. Facebook will combat COVID-19 misinformation more directly with notifications to users. *The Verge*, https://www.theverge.com/2020/12/15/22177085/facebook-covid-19-misinformation-notifications (2020, accessed 22 April 2021).

[26] Secretary DeVos Takes Historic Action to Strengthen Title IX Protections for All Students | U.S. Department of Education, https://www.ed.gov/news/press-releases/secretary-devos-takes-historic-action-strengthen-title-ix-protections-all-students (2020, accessed 7 April 2021).

[27] ISO - Members, https://www.iso.org/members.html (2021, accessed 22 April 2021).