Should users participate in governing social media?
Philosophical and technical considerations of
democratic social media
by Severin Engelmann, Jens Grossklags, and Lisa Herzog

Abstract
In recent years, a plethora of well-known data scandals has led to calls for alternative forms of social media governance. What challenges of institutional design would have to be met for developing meaningful democratic governance structures for a social media platform? Intertwining philosophical and technological considerations, this article explores the possibility and feasibility of democratically governed social media. We focus on the necessary technological requirements that guarantee secure voting for social media user participation. While we provide several arguments in favor of democratically governed social media from within, we argue that it should not be considered as an alternative to social media regulation from the outside.

Contents
I. Introduction
II. The case for democratizing social networks
III. Technical challenges of online voting in democratically governed social media
IV. The challenge of expertise
V. Conclusion

Introduction
When the relation between “social media” and “democracy” is discussed, the question usually is: what impact does social media such as Facebook, Instagram or Twitter — as it exists today — have on democratic processes? This question is urgent and important: if more and more political discourse takes place online, the ways in which it is shaped by the technical infrastructure gains weight. For example, by allowing the microtargeting of individuals with political advertisement that other users do not see, public discourse can be fragmented and public opinion can be manipulated (see Cadwalladr, 2018). Given the immense power of social media, however, one can also ask a different question about the relation between social media and democracy: what would it mean to turn a social media platform into a democracy, i.e., to govern it democratically? We here speak of “social media democracy” in a sense that goes further than giving users the possibility to vote on user content as a form of community-based content moderation. For example, platforms such as Reddit or Quora allow users to influence the visibility of user comments by so-called “upvoting” (making a comment more visible) and “downvoting” [1]. While such examples demonstrate that users already engage in some participative behaviors on social media platforms, we
address challenges of institutional design that would have to be met for developing meaningful democratic structures to really govern social media platforms like Facebook or Twitter democratically.

For example, Facebook is run as a corporation, with its founder, Mark Zuckerberg, in control of voting rights (Zuboff, 2019). Employees and users have hardly any voice in its strategic decision-making. In 2009, Facebook experimented with user deliberation and voting: It had set up a comment-and-vote governance system with the declared purpose of enabling user participation in its policy processes. But these attempts at participatory governance did not live up to procedural standards of democratic decision-making (Engelmann, et al., 2018). They were shut down in 2012, after the right to vote on Facebook policies had itself been put to a vote. Since a necessary quorum of 300 million voters was decisively missed (only 668,872 users voted), users effectively lost any participation rights.

When it proposed the termination of its participatory governance process, Facebook claimed: “We deeply value the feedback we receive from you during our comment period. In the past, your substantive feedback has led to changes to the proposals we made. However, we found that the voting mechanism, which is triggered by a specific number of comments, actually resulted in a system that incentivized the quantity of comments over their quality. Therefore, we’re proposing to end the voting component of the process in favor of a system that leads to more meaningful feedback and engagement.”[2] After this announcement, Facebook never implemented another participatory governance process. Following a plethora of privacy scandals and charges of having negligently enabled election manipulation (see e.g., Aral and Eckles, 2019), the question as to whether more stringent forms of social media governance are indeed possible and viable has gained global public interest. Some — including Zuckerberg — have openly supported the idea of an independent ‘Supreme Court’, tasked primarily with the specification of free speech and hate speech (Klonick and Kadri, 2018). Others have repeated the proposal to shift some power from the platform operator to social media users (Roose, 2018). However, since the termination of user participation in 2012, no tangible changes towards democratic forms of social media governance have been realized.

While our contribution cannot spell out a comprehensive account on the value of democratically governed social media, we here provide initial theoretical considerations about the value of democracy beyond the political sphere. Our account focuses on a necessary technological condition of, arguably, all democratically governed social media: how to ensure secure voting for social media user participation.

The benefits of social media platforms for users are obvious, which is why we expect them to stay. But if social media platforms are run as private corporations, a lot of power is concentrated in the hands of the owners. The interests of users, and of society at large, are insufficiently protected. National legislation, while certainly important, has difficulties controlling global structures like Facebook.

In reaction to public criticism, several large digital companies have invested various resources to establish initiatives with the purpose of addressing the ethical challenges of digital technologies (Bietti, 2020). Frequently lacking credibility as serious efforts to solve complex ethical challenges, such “ethics washing” has often been criticized as a toothless corporate communication and public relation strategy.

An alternative, and potentially more promising, strategy for holding those with power over social media platforms accountable is to govern them democratically. Below we discuss some arguments in favor of such democratic governance. But such a proposal immediately runs into questions about feasibility. Would democratic governance be practically possible? What technological infrastructure would it require?

Our paper has the following structure: In Section II, we justify the idea of governing social media platforms democratically, drawing on arguments from the recent debate about workplace democracy (e.g., Frega, et al., 2019) that can also be applied to social media companies, but with users as the main constituency. We then move to the question of feasibility, and, in Section III, intertwine philosophical and technical considerations. Here, we address challenges pertaining to voter individuation and manipulation of the voting process. In Section IV, we consider a second challenge of feasibility, which stems from expert knowledge, e.g., on different technical and financial options about which voters might need to make
Should users participate in governing social media? Philosophical and technical considerations of democratic social media

We argue that in addition to a technological infrastructure for voting, an epistemic infrastructure for deliberation and the transmission of information, involving groups like NGOs and external experts, would be needed. We conclude, in Section V, by briefly considering whether existing social media could indeed be turned into a democracy, or whether other social media networks, with more democratic governance structures, could emerge to replace it.

II. The case for democratizing social networks

Democracy can be justified on an intrinsic or an instrumental basis. From an intrinsic perspective, it is considered as the appropriate form of governance between individuals who consider each other as moral equals, because it expresses their equal standing and the equal respect they owe each other (see Saffron and Urbinati, 2013). From an instrumental perspective, democracy is considered to have certain positive consequences, such as the protection of individuals’ interests through the possibility of having a voice — as Sen (1983) has famously shown, democratic societies with a free press do not experience famines — or the ability of political systems to process knowledge effectively (e.g., Landemore, 2013). We here assume that while the intrinsic justification provides the most basic normative orientation, instrumental considerations need not and should not be neglected (see also Landemore, 2017). In other words, democratic governance structures should be designed such that we can expect reasonable outcomes, in particular by a careful division of labor between different institutions: courts and parliaments, expert committees and forums for citizen participation, etc.

Such an approach can also be applied to democratic governance structures beyond the political realm in the traditional sense, i.e., representation in parliaments at the local, regional and national level. There is a long tradition in political theory arguing for expanding the basic principle of democracy — if some people have power over others, they should be held democratically accountable, especially if important interests are at stake — into other spheres of life as well, e.g., the workplace and the media (e.g., Dahl, 1985) [3]. The vision of democracy that stands behind it sees it as a “way of life” (Dewey, 1927) that should be implemented in all social spheres, even if it may have to take on different forms, e.g., direct or representative, with different allocations of responsibilities to different constituencies.

In recent years, there has been renewed interest in such proposals, especially with regard to the workplace, with intense debates about the arguments for and against democratic governance in the economic realm (for an overview, see Frega, et al., 2019). While we cannot reiterate this debate in detail here, one point is worth noting: arguments in favor of democratic enterprises are often based on normative values, while arguments against them are based on practical considerations of feasibility, efficiency, or functionality. Hence, to win over opponents, defenders of workplace democracy or democratic governance of other social spheres need to come up with realistic proposals about how democratic governance could be made to work in such organizations.

One of the central arguments in favor of workplace democracy is the overwhelming power that economic entities, especially transnational corporations, have acquired in recent decades. This argument also holds for social media platforms: we see large concentrations of power, as a result of network effects that lead to almost monopolistic structures [4], in areas where important social goods are at stake. These goods are the privacy of users and the protection of online discourse from manipulation, especially, but not only, when it comes to political messages around democratic elections. This provides a prima facie case for democratic governance. The various scandals in recent years show that the current governance structures of social media are far from optimal and that there is likely room for improvement. Put differently: democratic governance for social media would not have to work very well in order to be still better than what we currently observe. Proposals for democratic governance are sometimes expected to be perfect and rejected if there is the slightest possibility of failure. But this means setting up an unfair standard of comparison, because the current governance structures are so far from perfect. For example, even if voters or their
Should users participate in governing social media? Philosophical and technical considerations of democratic social media

representatives were not fully involved in all decisions, some degree of involvement — if it goes beyond mere PR — could still be an improvement and could be the point of departure for further governance reforms.

One of the most interesting contributions to the recent debate on workplace democracy is Ferreras’ (2017) account of “firms as political entities.” She argues for a bicameral system in which both owners and employees of large companies are represented in chambers: one for capital, one for labor. For proposals to be accepted, they would have to have a majority of more than 50 percent in both chambers. This, Ferreras argues, would force both sides to come up with proposals that are acceptable for all, and that would be in line with the instrumental logic pursued by capital owners, but also the “expressive rationality” represented by workers, which emphasizes the quality and meaning of work. She puts this proposal into a historical line with other “bicameral moments”, from ancient Rome to the Glorious Revolution in Great Britain, in which a small elite of power holders had to accept sharing its power with the mass of the population. This, she argues, is the logic that the powerful owners of capital have to accept today: they need to share power with those who have to work to make a living.

We take it that this argument can also be applied to social media companies. But for them, the most important group whose interests are at stake are users, who share their data on the platform. Hence, users are the ones who should be given a democratic voice. Two arguments support this claim: 1) the risk of domination, and 2) the contributions of users. With regard to 1), recent scandals have made it very clear that users’ data and privacy are at risk of being abused by platform operators (Cadwalladr, 2018; Constine, 2019). Democratic participation by users is one of the tools that would help hold platforms accountable, to prevent such abuses. With regard to 2), there is a broad debate about the role that “free labor” plays for the digital economy. Social media platforms cannot operate without the contributions delivered by their users — this is, after all, what attracts other users and thereby creates the possibility for generating income from advertisement. This labor should be recognized by giving these “workers”, i.e., the users, some voice in the governance of platforms.

These arguments support the claim that there needs to be a “chamber” for users, in addition to one for capital. But employees should not be left out of the picture either; those are far fewer in number than users, but they have interests worthy of protection as well. Hence, a more complex model with more than two chambers could be envisaged. It could, for example, have one chamber for users, and a combined chamber for employees and investors, which in turn have sub-chambers that would have to agree to proposals. Alternatively, there might be three chambers for investors, employees, and users, respectively. Some questions might be decided by only one of these chambers; for example, questions about working hour flexibility and job rotation should be in the hands of the representatives of employees. Major strategic questions, in contrast, would have to be decided by all chambers together. In what follows, we focus mostly on the involvement of users, which raises specific challenges that the debate about workplace democracy has, naturally, not considered.

The chamber of users would be involved in all major questions of internal governance. In particular, users would be involved in all questions that concern their data: which third parties are given access to them, and under what conditions, what forms of aggregation and storage would be appropriate, how users could request deletion or correction of data, and other comparable questions. They would also have a say in decisions about the algorithms that govern user feeds, or about the kinds of advertisements that would be shown to users. Other questions, in contrast, should better be decided by court-like structures, for example by the “supreme court” suggested by some commentators that would adjudicate matters of hate speech. The protection of minorities, e.g., linguistic minorities, is another issue that should not be left exclusively to democratic decision-making, where they might be voted down. Instead, there could again be court-like structures to which minorities could appeal, or there could be ombudspeople to help find solutions.

A point worth emphasizing, in order to avoid misunderstandings, is that democratic governance within social media should not be considered as an alternative to regulation by political means from the outside, by means of public authorities and courts. Certain issues — for example, the way in which political
advertisements can be run on social media — concern not only users, but all citizens, and should therefore remain in the hands of national political and legal systems. Legal rules should standardly have priority over internal rules [7]. The delineation of issues that should be decided by internal democratic processes, and of processes that remain in the hands of political democracy at large, needs to be decided by the latter. The relation between social media’s internal democracy and national political democracies would thus resemble that between different levels of a federal system [8].

Democratic processes standardly involve phases of deliberation and of decision-making. Deliberation, however, can also take place in non-democratic organizations. It is the combination with voting that makes it a democratic practice: citizens deliberate in order to inform themselves, weigh arguments, and develop the preferences that they then express through their votes. Hence, voting is at the core of the democratic process; it is here that the idea of “the power to the people” really finds its expression. To be sure, democracy cannot be reduced to voting — this would suggest an overly narrow understanding of democracy and its values. Different theories of democracy (deliberative, epistemic, agonistic, radical, etc.) have emphasized the role of public discourse, of the aggregation of the ‘knowledge of the many’, or of non-discursive forms of dissent and protest. But we take it that these dimensions of democracy should not be understood as replacing voting procedures. Voting on the basis of equality — one person, one vote — remains a core feature of democracy, however it is understood.

In what follows, we therefore focus on some of the technical and epistemic challenges that would have to be overcome to develop meaningful voting procedures for social media platforms like Facebook or Twitter. We ask whether such a proposal could be feasibly implemented, in ways that could potentially live up to the democratic principles that motivate the proposal for democratic governance.

III. Technical challenges of online voting in democratically governed social media

Online voting enables remote voting and promises to increase participation and reduce election costs (Schaupp and Carter, 2005). Any form of democratic participation requires a voting procedure. History amply demonstrates that for all democratic processes, there are those who try to protect their integrity, and those who attempt to undermine them. Thus, all voting procedures must fulfill certain criteria that ensure the overall integrity of the election. There is no reason to think that the battle between election protection and election manipulation would not affect voting in democratically governed social media.

An online voting system can take a number of different forms, depending on the tailoring of the constituencies, the nature of the election (e.g., single winner versus multiple winners), and other design decisions. The main question we raise here pertains to the necessary security measures of online voting in social media. We take it that without reasonable security measures, online voting would be meaningless. It would be open to manipulation and its democratic promise would thus not be credible, discouraging participation. In this section, we outline the most relevant security decisions election officials would need to consider when setting up an online voting system in the context of social media.

Security measures for online voting can be divided into two main components: in a first step, the process typically needs to ensure that only voters that fulfill pre-specified eligibility criteria can cast their vote (registration verifiability). In a second step, the online voting process typically adds further verifiability guarantees, for example, allowing voters to verify whether their vote is 1) cast-as-intended, 2) recorded-as-cast, and 3) tallied-as-recorded. For this second step, computer scientists have made progress developing so-called end-to-end (E2E) verifiability of online voting processes (see Ryan, et al., 2015). E2E enables every individual voter to audit the entire voting process — a feature that is usually not possible in paper-based offline elections. In other words, users can verify that their vote has been cast and recorded correctly as well as that their vote (and everyone else’s) has been correctly tabulated. In the next subsection, we discuss how to achieve secure voting for the context at hand.
We take it that online voting, rather than being done on platforms themselves, should take place via an external server infrastructure. Voter registration should consist of a combination of the social media user profile ID and the national passport ID of the voter. Moreover, public verifiability of the voting process should make us of pseudonymization but not E2E verifiability.

**Determining and individuating the set of eligible voters**

The first step in online voting is to determine the set of eligible voters, *i.e.*, social media users. Eligibility checks presuppose 1) the design of constituencies and 2) the selection of eligibility criteria. At first glance, one might think that voters could register to vote by using their user profile ID, for example their social media platform ID, which is a unique sequence of numbers that connects to a single social media profile. Verification of a Facebook user profile, for example, is based on a unique user profile ID linked to a single e-mail address, and other platforms operate in the same way. This opens the door to election manipulation since one user can have many e-mail addresses each associated to a single social media account. Both from “outside” and from “within” the social media platform it is nearly impossible to verify that an individual only used their “real” and not any of their “fake” accounts to cast a vote. To prevent multiple votes, an online voting system — just like any paper-based vote — requires a procedure that distributes unique identifiers to eligible voters.

Registration of a vote in the context of social media requires a verification method to ensure that there is a human voter behind each single social media profile. There are various challenges to ensuring this: profiles run by companies or other entities would, presumably, have to be excluded; profiles generated by bots, *i.e.*, automated systems that emulate the behavior of human users, would also have to be excluded; humans with several profiles would be allowed to vote with only one of them.

As to the first challenge (profiles run by companies), it is noteworthy that Facebook, for example, offers two kinds of accounts: personal profiles and fan pages. Many organizations run fan pages, which can have unlimited amounts of followers, while personal accounts can have a maximum of 5,000 “friends”. A first step would be to only give voting rights to personal accounts. One might ask whether organizations or individuals that run fan pages should also have the right to participate in elections — maybe as a separate constituency, with representatives who have a say on certain topics but not others. We here bracket this question, but point to a challenge that nonetheless remains: given the influence of entities with fan pages on discussions on social media, as a sheer question of numbers, would their influence have to be regulated during election times? For example, wouldn’t it be problematic if a discussion about the respective rights of users and advertisement companies took place on the fan page of a company that had itself a stake in the issue? But where should one draw the line here, and who would make decisions? It might be suggested that spaces for deliberation could be offered by fan pages run by independent bodies, which enforce clear and transparent policies for commenting. This seems feasible in principle, but requires additional steps to ensure the integrity and neutrality of these forums. Finally, to enable the largest degree of diversity in discussion and policy framing, debates will probably need to shift to external platforms, too.

The second challenge concerns profiles run by bots. In the first quarter of 2019, Facebook claimed to have removed almost 2.2 billion fake accounts from its platform — almost the same amount as that of active user profiles at the time (2.38 billion) (Yurieff, 2019). Therefore, a central effort in protecting the integrity of social media elections would have to be the assurance that bot profiles cannot register for a vote. For this task, captchas (completely automated public Turing tests to tell computers and humans apart) are commonly used to effectively differentiate humans from automated computer programs such as bots (von Ahn, *et al.*, 2003). Recently, a research team successfully broke all text-based captchas deployed by the top-50 most popular Web site (Ye, *et al.*, 2018). Their method relied on a machine learning-based generative adversarial network that produces a generic text-based captcha solver. However, more advanced types of captchas such as image-based, video-based, audio-based, puzzle-based or a combination of captcha types could provide enough shielding from malicious bot voter registration (Singh and Pal, 2014).

If captchas eliminated the threat of bot participation, one would have to decide about a third challenge:
Should users participate in governing social media? Philosophical and technical considerations of democratic social media

whether the risk of human-based double voting is acceptable. If deemed unacceptable, then a system will need to provide unique identifiers. Since a social media platform ID on its own cannot serve as a unique identifier, determining and individuating voters in an online election depends on additional criteria associated with the design of the constituencies. For example, electing a representative for every 100,000 users in a designated region could imply registration by IP address. As IP addresses are dynamically assigned this would allow users to travel digitally into the designated area to cast their vote. For example, the use of virtual network privacy technologies (VPNs) potentially enables voters from other regions to participate in the election of another constituency. Thus, IP addresses cannot provide the necessary guarantees to protect against the participation of non-eligible voters.

National affiliation associated to a unique ID (for example, a passport ID) in combination with a user profile ID could determine and individuate the set of eligible voters. This is how the Estonian I-Voting System verifies the identity of voters for local and national elections (Alvarez, et al., 2009). Estonians use a smart identity card that can perform cryptographic functions to make legally binding decisions on official government Web sites. As an alternative, Estonians can also use a so-called Mobile ID — a smart mobile SIM card that can perform the same functions as the smart identity card but does not require a smart card reader [10]. This demonstrates that building constituencies by national affiliation can in principle provide a secure method for user registration. Consequently, an official election server would need to match an individual’s stored national ID with her user profile ID (both encrypted). Here, two competing solution approaches should be discussed: using the social media’s own server infrastructure or an external server infrastructure.

The former solution would entail voters having their passport IDs stored on servers run by the social media company. This approach would likely undermine the credibility of the election process. During Facebook’s past attempt to run its platform democratically, a large voter base orchestrated an attempt to move election components to a third-party platform (Engelmann, et al., 2018).

The Estonian government publicly advertises bids for server solutions prior to every election [11]. This allows governments to make demands on the election server infrastructure and prevents contracts that give one company permission to collect, process, and store election data for multiple elections. Moreover, in Europe, data protection authorities (DPAs) could serve as the official election authorities and select a particular server/software infrastructure from bidding offers. European DPAs are independent authorities that supervise the application of data protection law (i.e., General Data Protection Regulation, GDPR) [12]. Individuals would need to verify themselves to servers selected and monitored by the DPAs. The entire election process could eventually receive a “seal of approval” by the DPA certifying that the election process and outcome are binding under the terms of the GDPR. Since each member state has its own DPA, each member state could represent a constituency with the country’s DPA playing the role of the election authority. Finally, the European Data Protection Board (consisting of DPA representatives from each member state) could work towards ensuring equal election standards across all member states. For countries outside of the European Union, other sufficiently independent bodies, which have the necessary technical competence and are perceived as credible by citizens, would have to play a role analogous to that of the DPAs.

Verifiability of the voting process

Generally, in any voting system significant efforts need to be invested to ensure both secrecy of the ballot and verifiability of the voting process. If a voting system were not required to provide secrecy of the ballot, voters could verify the correctness of the voting process themselves. Since secrecy would not be necessary, each voter could simply check whether their vote was cast, recorded, and tallied correctly on a Web site listing all votes publicly. This, however, would put voters at risk of voting coercion, which would seriously undermine the legitimacy of the election. As Hilbert [13] puts it: “Theoretical reasons behind the secret ballot turn out to be some of the trickiest challenges of reaping the benefits of a real e-democracy.”

Thanks to cryptographic proofs, online voting can — in principle — provide auditing guarantees to voters
Should users participate in governing social media? Philosophical and technical considerations of democratic social media

(Schaupp and Carter, 2005). Paper-based elections commonly apply eligibility safeguards to ensure that only those can cast their vote that are entitled to do so (as discussed above). Since voters use a paper form to cast their vote, they have some assurance that voting guarantees cast-as-intendent. However, after casting their ballot, voters need to trust voting officials to conduct the remaining procedures correctly, for example, to make sure that the vote is recorded-as-intended and tallied-as-intended. Novel Internet voting systems enable E2E verifiability, which allows any voting participant to verify the entire election process without revealing the transaction of their vote to any third party (Ryan, et al., 2015). Through E2E, voters can get mathematical proof that their vote has been cast-as-intended, recorded-as-casted, and tallied-as-intended. In online voting, such auditing measures are highly valuable since remote voting often means that critical voting infrastructures can be attacked from multiple gateways. In 2014, a team of researchers implemented several undetectable client-side and server-side attacks on a reproduced setup of the Estonian voting system, which does not implement E2E (Springall, et al., 2014). Similar attacks were modelled on New South Wales’ iVote System in a 2015 state election in Australia (Halderman and Teague, 2015).

Numerous different approaches to E2E have been suggested (Chaum, et al., 2005; Chondros, et al., 2016; Culnane and Schneider, 2014). For example, an advanced commercial product called Scantegrity II uses a cryptographic technique called “divide and choose” which enables zero-knowledge proofs [14]. Such proofs can demonstrate that a certain statement is true, e.g., “the voter’s ballot has been tallied-as-intended”, without revealing the content of the transaction (guaranteeing secrecy of the ballot). While E2E is a desirable property for an online voting system, current solutions lack user-friendliness for both election officials and voters. For example, to implement Scantegrity II, voters require a special pen with invisible ink to print a hidden three-character code that serves as a cryptographic marker. This three-character code must be entered on a public Web site where voters can verify that their ballot was recorded-as-intendent (Chaum, et al., 2008). Overall, no current commercial E2E solution features the necessary robustness for application in a political election [15], and there are no E2E voting systems that enable multiple winners (Chondros, et al., 2016).

A more feasible approach could rely on publishing pseudonymized identifiers for each voter along with their ballot choice on a Web site. After each individual has cast their ballot, the election authority (e.g., the DPAs in Europe) assigns and sends an encrypted pseudonym to each voter. The DPA then posts all pseudonymized names together with the voted option on a publicly accessible bulletin board. Now, every single voter can look up their pseudonym to verify that their vote has been correctly recorded. Moreover, everyone can check if the tally has been correctly tabulated. The downside of this approach is that voters need to rely on other voters to check that their votes appear correctly, because each voter can only verify their own vote. Also, while a pseudonym reduces the chance of a natural person being identified from “outside”, a malicious election authority (generating the pseudonyms) may compromise the secrecy of the ballot from “within” (Benaloh, et al., 2015).

To be sure, such issues compromise political elections as well. One might hold that the stakes in elections on social media platforms are not sufficiently high to justify such extensive worries about the verifiability of the voting process. On the other hand, the very point of such a process would be to ensure trustworthy governance structures; if users have doubts about the integrity of the voting process, this might discourage participation.

The process described above would protect social media elections against multiple votes cast by a single voter. However, it must be mentioned that new challenges, on a practical and political level, follow. There is, first, a question of cost: who would provide the funds for this election infrastructure? Second, there is a question about what to do in countries in which such institutions are lacking, or are not sufficiently trustworthy. Should social media users from such countries be registered on servers in different countries? Would this be perceived as trustworthy, or as a problematic form of technological neo-colonialism? Third, there is a question about equal access, even within countries: while in some countries, almost all citizens have a passport or ID card, in others this is not a common practice; those who hold passports are, most likely, to come from more privileged backgrounds (they can more easily afford the fees, they are more likely to need the passport for international travel, for example). Moreover, some countries have
Should users participate in governing social media? Philosophical and technical considerations of democratic social media

considerable groups of undocumented populations, e.g., undocumented migrants. Should these groups be excluded from elections on social media? If one relies on state infrastructure for organizing voter identification, this seems an unavoidable implication. Whether or not this is acceptable, or whether other mechanisms for identifying such voters could be used, would probably have to be decided on a case-by-case basis.

But a voting process, even a highly secure one, continues to draw its value from the fact that it reflects the preferences of voters. These preferences should, ideally, be well-informed — a challenge for all democratic processes and a particular challenge for a democratically governed social media. In the next section, we turn to the problem that users might simply be too uninformed, and maybe even unwilling to inform themselves.

---

**IV. The challenge of expertise**

As the previous section demonstrates, thinking about governance structures for a social media platform requires technical expertise. This also holds for many other questions that the voters in a democratically governed social media would have to decide about: questions about security standards, about privacy, about the relation between the rights of users and of other constituencies, e.g., advertisers.

The collection, processing, and analysis of data from personal profiles is a complex process. Understanding the various options of how these processes can be designed requires not only technical knowledge, but also an understanding of their financial dimensions. This raises questions about the competence of voters: would they be competent enough to make meaningful contributions to such decisions? Would they make the effort to educate themselves about relevant alternatives? Would they even know what they would be voting upon? If not, why should they get involved at all?

For example, one area that requires expertise are the complex data sharing practices contained in privacy disclaimers and consent forms. When subjecting novel data practices to a vote, privacy experts would need to translate the privacy implications to a broader public. For example, Facebook aims to integrate user information between businesses belonging to the Facebook group (historically, this has already occurred with Instagram which was subjected to a vote in Facebook’s first attempt to govern its platform “democratically” in 2009). How are such data sharing practices communicated in an updated privacy disclaimer? More importantly, what advantages and disadvantages does the sharing of information between businesses belonging to the same group have for users?

More generally, experts need to be able to simplify the affordances of various digital technologies relevant to the social media context, such as ID-based cross-device user tracking or image-understanding tools generating inferences based on users’ shared visual data (to name just two examples). Users would require such knowledge, for example, to vote on the much debated issue of providing transparency regarding how their data is turned into inferences that bear economic value. In this context, a recent study by Andreou, et al. (2018) emphasizes the persistent lack of transparency in the use of data subjects’ information for micro-targeting.

Such challenges of voters’ competence impact democratic elections in other areas as well, with some commentators (e.g., Brennan, 2016) calling for “epistocratic” alternatives to democratic decision-making. Here we cannot go into this general debate, but will rather focus on arguments that could be applied to a democratically governed social media. The problem of expertise can be understood as a feasibility challenge: without a satisfying answer to it, introducing formally democratic structures might be quite meaningless. Even if information about many technical questions were made transparently available, it would probably be too hard to digest for laypeople. At the same time, one cannot expect citizens to become themselves experts on all the issues that concern them — this is already a challenge for political democracy.
Adding democratic structures on social media platforms would presumably risk increasing this cognitive burden.

However, as Mansbridge, et al. (2012) have pointed out, one needs to understand public deliberation, and the ways in which it processes knowledge, from a systemic perspective: different individuals, groups, and institutions play different roles, and there is a division of labor. Experts can be integrated into democratic decision-making in various ways, without falling into a technocracy. As Christiano (2012) argues, the mechanisms that can be used to integrate expert knowledge into the decision-making processes of politicians and lay people include solidarity between experts and other groups, overlapping understanding between different groups (e.g., economists and public policy experts) who can “translate” expert knowledge into more accessible forms, competition between parties that creates incentives to point out flawed knowledge on the other side, and sanctions (e.g., loss of reputation) for experts who abuse their knowledge.

In other words, the integration of expert knowledge into democratic processes presupposes a complex ecosystem of formal and informal institutions, with mutual checks and balances. Can one imagine such an ecosystem to arise around the democratic governance of a social media platform? In the case of Wikipedia, many forms of relevant expertise — on the technical level, but also on the level of content and on the level of management — have been quite successfully integrated into a governance structure that is if not democratic in the sense discussed here, at least quite different from corporate structures and explicitly oriented towards the public good. It is fascinating to see how much voluntary labor, including the labor of technical experts, is harnessed to keep Wikipedia up and running.

Similar networks and structures would, presumably, be needed for creating the informational ecosystem that would give users sufficient information for their votes to be meaningful [16]. It is likely that various parties or platforms would form, which would specialize on certain issues, e.g., privacy protection or information manipulation. There might also be platforms that combine value decisions — e.g., on the question of privacy vs. advertisement income — with the relevant technical expertise for putting the envisaged values into practice. If such an ecosystem is in place, individuals can delegate many decisions to agents they trust, for example by voting for platforms or parties that share the same values and that have incentives to find the best available expertise on the relevant topics.

Here, one challenge is the independence of experts. Tech companies, including social media platforms, are keen to hire the “best and brightest” of data science graduates, and they can offer higher wages than, say, an NGO with the goal of providing independent analyses of social media policies. A similar problem had been discussed after the Great Financial Crisis of 2007: financial market expertise — especially expertise in complex financial products and their effects on markets — was concentrated in investment banks rather than regulatory bodies. Arguably, this was one factor that made it so hard to anticipate what was happening before the crisis hit. The current situation of data scientists is structurally similar: as a community, they have insider knowledge that is of enormous importance for society and that can be used in beneficial or harmful ways. Recent calls for ethical codes for data scientists respond to this constellation (e.g., Eubanks, 2018).

In the context of democratically run social media, such codes would certainly not harm, but they might not be sufficient. Instead, what one would hope for would be processes of open and critical contestation in which expert knowledge is debated, and in which lay people, while not understanding all details, can get a reliable sense of what is at stake and what different parties stand for. For this to come about, various agents could play a role: academic researchers, activists, but also tech journalists and educators. Independent bodies, run as foundations, could help to bring different individuals together and create synergies between them. Formats such as “mini publics” may evolve, in which randomly selected members of the voter base deliberate together and can ask questions to experts. All in all, creating an informational ecosystem that would make sufficient voter competence possible would be a challenging, but by no means an insurmountable task.
V. Conclusion

In this paper, we have outlined the basic steps for establishing a democratically governed social media. We have argued that whenever there are large concentrations of power and important goods at stake, democratic governance can be justified on the basis of both intrinsic and instrumental reasons. Relying on Ferreras’ (2017) account of “firms as political entities”, we have argued that a social media governance structure could consist of a tri-cameral system representing investors, users, and employees. While we provide several arguments in favor of democracy from within, this should not be considered as an alternative to regulation by political means from the outside, by means of public authorities and courts, a point that is also confirmed when one considers the technological preconditions for meaningful democratic governance, which partly depend on outside structures.

Next, we have laid out the necessary technological preconditions to guarantee the most basic form of democratic participation: voting. Overall, we argued that online voting should take place via an external server infrastructure, to ensure that voting data cannot be accessed by the social media platform or the state. Both voter individuation and registration should consist of a combination of social media ID and national ID of the voter. Moreover, while end-to-end verifiability of the voting process is a desirable feature, distributing pseudonymized identifiers for each voter and publishing their ballot of choice on a public website is a more feasible approach. Having a democratic governance structure and a technologically-mediated voting system in place alone does not, however, guarantee the success of democratically governed social media. Laypeople must acquire at least basic voting competence to understand how different outcomes impact their online life. Here, we suggested social institutions like NGOs, or more generally independent bodies of experts, to engage in a technical knowledge transfer as part of a public discourse.

As these considerations show, designing a democratic governance structure is not straightforward — but neither is it impossible. Political theory can deliver ideas about mechanisms, drawing on the history of political thought and political practice, e.g., in ancient Greek democracy, to think about the strengths and weaknesses of different institutional solutions. Technical expertise is needed to understand the challenges and the possibilities of implementation. As the proposals for how to implement democratic voting on a social media platform discussed above demonstrate, technical expertise would also be needed for realizing and monitoring elections, and for updating the institutional structures when new research insights or technological developments unfold.

A second kind of challenge, however, concerns the transition: is it even conceivable that social media “as we know them” would make a transition towards democratic governance? Would its current business model, which is basically driven by advertisements and offers of “free” services for users, be compatible with democratic governance, or would it have to find other sources of income? It is clear that much would depend on whether sufficient political pressure could be built up to guide such a transition. This is unlikely in the current political and ideological environment, but might come faster than expected if the political winds, especially in the U.S., would shift towards more consumer protection. Arguments that social media platforms need to be turned into public infrastructures have already been brought forward (e.g., Rahman, 2018). If this were the case, democratic governance structures, rather than top down rule by government bureaucrats, might appear as the more attractive option.

Another scenario would be a more market-based transition: if democratically run social media platforms were to come into existence, users might shift towards them. At some point, they might reach a critical point at which mass migration would take place. This is not a new hope and it is not clear how likely it is to be fulfilled, given the strong network effects that existing platforms often maintain. But it is well conceivable that a sinking reputation of, for example, Facebook could prepare such a shift.

Finally, it is worthwhile to ask the question of what a democratically run social media platform could look like, and which technical and epistemic challenges it would have to overcome. Addressing these issues requires interdisciplinary collaboration, and it would be desirable to have various design options on the
About the authors

Severin Engelmann is a Ph.D. student at the Professorship for Cyber Trust at the Technical University of Munich (Department of Informatics). With a background in philosophy of technology and computer science, Severin Engelmann’s research investigates the normative dimensions of large digital socio-technical systems. In particular, he studies how social media platforms and social credit systems (e.g., in China) can become more transparent and accountable.
ORCID: 0000-0001-8368-4484.
E-mail: severin [dot] engelmann [at] tum [dot] de

Prof. Jens Grossklags holds the Professorship for Cyber Trust at the Department of Informatics at the Technical University of Munich. He studies security and privacy challenges from the economic and behavioral perspectives with a variety of methodologies. Prof. Grossklags received his Ph.D. from the University of California, Berkeley and was a Postdoctoral Research Associate at the Center for Information Technology Policy at Princeton University. He then directed the Security, Privacy and Information Economics Lab, and served as the Haile Family Early Career Professor at Pennsylvania State University.
ORCID: 0000-0003-1093-1282.
E-mail: jens [dot] grossklags [at] in [dot] tum [dot] de

Prof. Lisa Herzog, D.Phil., is a professor at the Department of Ethics, Social and Political Philosophy at the University of Groningen. Her research focuses on economic democracy, political epistemology, and ethics in organizations, drawing on the history of ideas, but also addressing contemporary issues. Prof. Herzog received her Ph.D. from the University of Oxford as a Rhodes Scholar in 2011, and has since then worked at the universities of St. Gallen, Frankfurt, Stanford, and the Technical University of Munich.
ORCID: 0000-0001-9348-1154.
E-mail: l [dot] m [dot] herzog [at] rug [dot] nl

Acknowledgements

We would like to thank First Monday’s anonymous reviewers for their helpful and constructive reviews of our contribution. We also thank the participants of the Philosophy Colloquium of the Department of Philosophy at University of Helsinki as well as the participants of the 2019 Henry Tudor Memorial Address at the Center for Political Thought, University of Durham, for their valuable comments on our contribution.

Notes


3. Of course, such models have only very partially been realized (e.g., to some extent, in the German codetermination model or in cooperatives). Most traditional media were (and continue to be) organized as capitalist firms. For reasons of scope, we here cannot engage in the debate about why this is problematic and what alternative models of media governance could look like.
This problem might be reduced if one could impose demands of interoperability and/or portability of profiles on social media companies. This would create meaningful “exit” options, allowing users to “vote with their feet” and thereby reducing the need for “voice” (Hirschman, 1970) But it is not clear whether such an option would be politically feasible, especially across national jurisdictions. Even if it did, users would still only have the option to submit to one type or other of non-democratic organization. Nonetheless, such a strategy would be a promising way of reducing the power of social media platforms, and it could also be pursued in combination with internal democratization.


Depending on the business model of a democratically run social media, one might also consider adding other groups, e.g., those who advertise on social media. The rationale for including them would be the question of whether or not they stand in relations of dependence on social media like Facebook and cannot easily exit these relations. Whenever this is the case, groups should have some voice in the governance process. In some cases, however, it might also be sufficient to give them a consultative role.

There might be difficult questions concerning countries that are not democratically governed, but that is a topic too broad to be addressed here, and it is a problem for social media whether it is run democratically or by its owners alone.

Would it also make sense to think about federal structures inside social media? For example, some issues might be decided differently in different countries in accordance with local cultures. Consideration for such specificities might, however, be in tension with the point of social media being a global network, which by definition needs to regulate certain issues on a global level. We acknowledge the possibility of federal structures, but for reasons of space do not discuss them in detail.


In addition, large components of the server software are made transparent for public scrutiny via GitHub.


See for example the FAQs of Helios, another online voting system, at https://heliosvoting.org/faq, accessed 22 January 2020: “Should we start using Helios for public-office elections? Maybe US President 2016? No, you should not. Online elections are appropriate when one does not expect a large attempt at defrauding or coercing voters. For some elections, notably US Federal and State elections, the stakes are too high, and we recommend against capturing votes over the Internet. This has nothing to do with Helios itself: we just don’t trust that people’s home computers are secure enough to withstand significant attacks.”

Running social media democratically would also mean that voters — or at least their representatives or ombuds people — would have to get access to information that is currently treated as business secret. How exactly to organize the flows of information would have to be a matter of public policy, because it would have implications for the structures of competition in the market for social media platforms. While this would certainly be a source of resistance from the perspective of social media like Facebook, we take it that it would be potentially desirable to open up at least some forms of knowledge currently held exclusively by Facebook.
References


Should users participate in governing social media? Philosophical and technical considerations of democratic social media


Should users participate in governing social media? Philosophical and technical considerations of democratic social media


Should users participate in governing social media? Philosophical and technical considerations of democratic social media
*First Monday*, volume 25, number 12 (December 2020).
doi: [https://dx.doi.org/10.5210/fm.v25i12.10525](https://dx.doi.org/10.5210/fm.v25i12.10525)