Canadian Journal of Philosophy (2022), 1–16
doi:10.1017/can.2022.4

ARTICLE

What Makes Personal Data Processing by Social Networking Services Permissible?

Lichelle Wolmarans[1] and Alex Voorhoeve[2]*

[1]PUBLIC, London, UK and [2]Philosophy, Logic and Scientific Method, London School of Economics and Political Science (LSE), London, UK
*Corresponding author. Email: a.e.voorhoeve@lse.ac.uk

Abstract
Social networking services provide services in return for rights to commercialize users' personal data. We argue that what makes this transaction permissible is not users' autonomous consent but the provision of sufficiently valuable opportunities to exchange data for services. We argue that the value of these opportunities should be assessed for both (a) a range of users with different decision-making abilities and (b) third parties. We conclude that regulation should shift from aiming to ensure autonomous consent towards ensuring that users face options that they will use to advance individual and common interests.

Keywords: Consent; personal data processing; privacy; autonomy; contractualism

1. Introduction

Social networking services (SNS) are online platforms that enable individuals to expand their social relations to the online environment (Vallor 2015), for example by connecting with potential employers on LinkedIn, engaging in political debates with strangers on Twitter, or staying up to date with relatives through Facebook. SNS offer a service through which users can build a digital identity, develop relationships, and access opportunities and media. They are also a gateway to a range of goods, services, and applications. SNS typically offer access to their platforms in exchange for the opportunity to collect, process, use, and commercialize users' personal data (or "process personal data," for short).

In this paper, we investigate under what conditions this exchange is permissible. We employ the definition of personal data given in the European Union's General Data Protection Regulation (GDPR), which defines personal data by whether a piece of information gives an actor the ability to identify an individual. Specifically, it defines it as "information relating to (…) [a] natural person (…) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (European Parliament and the Council of the European Union 2016, art.4, cl.1). This includes both information that users voluntarily provide and information generated by their online activity.

This definition is inclusive: an identifier can cover everything from a person's medical history to the fact that they like the TV series *Desperate Housewives*. Naturally, the processing of such diverse pieces of information will not always affect important interests of the individual to whom the data pertains, nor need socially important issues always be at stake. The GDPR therefore recognizes

special types of personal data where important individual and societal interests are likely to be at stake, including data about a person's ethnicity, political opinions, religious or philosophical beliefs, health, sex life, and sexual orientation, as well as genetic and biometric data (European Parliament and the Council of the European Union 2016, art.9). Still, the GDPR's capacious definition is useful because, with big data algorithms, even apparently trivial pieces of information about an individual can be used to predict a range of sensitive personal information. For example, in one large sample, liking *Desperate Housewives* on Facebook was indicative of being gay (Kosinski, Stilwell, and Graepel 2013).

Personal data is processed by a range of institutions for a multitude of purposes. To keep our discussion manageable, we focus on the exchange between users and SNS. Five characteristics of this exchange motivate this focus. First, SNS influence nearly every aspect of users' lives, from relationships, purchasing behaviour, job opportunities, and exposure to news and opinion. Second, as we shall explain, the exchange is one in which people are prone to a host of decision-making biases. Third, users often provide extensive personal data to SNS. Fourth, the processing and monetisation of such data is a centrepiece of the SNS business model. Finally, the markets in which SNS operate are highly concentrated. Along with SNS' vast resources and knowledge, this ensures the relationship between users and SNS is characterized by grave imbalances of power. Our conclusions will generalize, we hope, to contexts with similar characteristics, such as using search engines, online gaming, and transacting in the metaverse.

We start from the premise that users typically have important interests in exercising control over at least a significant part of their personal data. We focus on privacy interests. These include users' abilities to (i) manage their accessibility to others and the degree to which they are the object of their attention (Gavison 1980); (ii) establish and maintain intimate relationships, which are partly defined by the exclusive sharing of personal knowledge (Rachels 1975); (iii) control their self-presentation in contexts ranging from the intimate to the job market; (iv) avoid market-based harms that come from others knowing information that may enable them to charge higher prices for goods or services (as, for example, health status may impact access to travel or life insurance; see Acquisti, Taylor, and Wagman 2016); and (v) to avoid risks of discrimination, harassment, and other harms that occur when others target them for their personal characteristics. While these categories call to mind each person's interests to control their personal data, there are also important interests that others have in a person's disclosure of data because one person's disclosure may permit inferences about others. Moreover, there are collective interests in the rules governing the transfer of personal data, including the way that such transfers contribute to concentrations of economic and social power and how they shape democratic discourse (Véliz 2020; Benn and Lazar 2022).

According to the Privacy Self-Management paradigm, the decision of how much personal information to cede control over to an SNS in return for the envisioned benefits provided should be up to the data subjects (Solove 2013; Bowman and Mathews 2018; Warner 2019). The privacy policy of an SNS outlines which forms of personally identifiable information can be collected, how this data is stored, and how it may be used and shared. Users are held responsible for agreeing to this policy, either implicitly or explicitly, when accessing services. Users have control over privacy settings and the voluntary disclosure of information. On this view, the consent of the user plays a large role in justifying the personal data processing practices of SNS. Within wide boundaries, it is taken to be sufficient to make the collection and use of personal data both legally and morally legitimate (Solove 2013).

However, this approach has been extensively criticized (see e.g., Solove 2013; Barocas and Nissenbaum 2014). The following cases illustrate some of the questions about the conditions under which these exchanges take place.

Cambridge Analytica: In 2014, Global Science Research launched an app on Facebook which paid users to take a personality test for "research purposes." The app harvested the profile data

and private messages of its 270,000 users and their Facebook friends, for an estimated total of 72 million users. The personal data was transferred to Cambridge Analytica and used to develop targeted political ads. Global Science Research's access to this data was in line with Facebook's privacy policy at the time, to which users had agreed. However, users of the personality test app complained that the purposes to which the data were put were beyond what they intended, and those who were merely Facebook friends with the app's users complained of an invasion of privacy, since they had no inkling that their "private messages" could be harvested in this way (Bowcott and Hern 2018; Rosenblatt 2019).

Grindr: In 2018, it emerged that Grindr, the largest SNS for the LGBT+ community, sold data on users' HIV status, sexual preferences, and location to third parties. This data could be used to embarrass or disadvantage Grindr's users, for example in accelerated underwriting, which permits the use of social-media data for the pricing of life insurance, unbeknownst to the purchaser (Scism 2019). There were complaints that the sale of data to third parties was buried in complex terms, that default settings on the app induced users to transfer too much data, and that there was no possibility to use the service whilst declining the onward sale of one's data (Singer 2018; Norwegian Consumer Council 2018).

Instagram: Facebook, the parent company of Instagram, has conducted internal research on the effects of Instagram use and the targeted ads that it exposes users to. This research suggested that for a subset of users, including young women and teenage girls, Instagram use is an important contributor to feelings of inadequacy, especially about their bodies, and to depression. The company did not publicly disclose this research (Wells, Horwitz, and Seetharaman 2021).

In the Cambridge Analytica and Grindr cases, critics have claimed that users' privacy was violated, and their data put to uses that risked significant setbacks to their interests and to collective goods. The response from Facebook and Grindr has been that users had consented to how their data was collected, shared, and used and that they should have been aware that their data could be accessed by third parties since Facebook and Grindr are public fora and selling users' data is standard practice (Singer 2018; Rosenblatt 2019). In the Instagram case, critics have argued that Facebook should have disclosed its research indicating a risk of harm before seeking users' consent to processing their data. Facebook responded that the research was insufficiently advanced (Wells, Horwitz, and Seetharaman 2021). Our aim in this paper is to evaluate these critiques and industry responses. We aim to establish what, if anything, is wrong with current practices based on the Privacy Self-Management paradigm and what, if anything, would have to change to make exchanges of personal data for services permissible. We proceed by considering two rival answers. In section 2, we consider the Autonomous Authorisation (AA) account, which holds that SNS require users' autonomous consent to avoid infringing users' rights over their personal data. On this view, the problem with existing consent regimes is that SNS often fail to secure such consent and the solution is to require that they do secure it. In section 3, we reject this account. We argue that it would impose undue barriers to access. We also argue that it fails to adequately account for the power imbalance between users and SNS and for the social effects of individual exchanges. In section 4, we outline Scanlon's Value of Choice (VoC) account, on which such transactions are rendered permissible by the provision of sufficiently valuable opportunities to exchange access to personal data for services. On this view, the problem with existing consent regimes is that SNS often fail to provide sufficiently valuable opportunities to users. In section 5, we argue that the VoC account avoids the shortcomings of the AA account. We conclude in section 6.

2. Autonomous authorisation

Theories of valid consent outline the conditions that are both necessary and sufficient for consent to an act to be morally transformative in the sense of it being the case that the consenter has no claim against the act precisely because they offered their consent (Feinberg 1986, 177–78; Thomson 1990, 348; Kleinig 2010; Miller and Wertheimer 2010; Dougherty 2020). One leading theory of valid consent is the version of the AA account put forth by Ruth Faden, Tom Beauchamp, and James Childress (Faden and Beauchamp 1986; Beauchamp 2010; Beauchamp and Childress 2019). On this version of the AA account, consent is morally valid just in case it constitutes an autonomous authorization, which is taken to involve that the consenter: (i) has sufficient information and appropriate understanding of the possible consequences of giving their consent; (ii) is a competent decision-maker; (iii) consents intentionally; and (iv) consents freely (Beauchamp 2010).

While this view has its origin in bioethics, it is widely recognized as having application in nonmedical contexts, including in the digital realm (Feinberg 1986; Miller and Wertheimer 2010; Edenberg and Jones 2019). In the biomedical context, it starts with the assumption that patients have rights over their bodies and minds which are infringed unless morally valid consent is obtained. It thereby protects patients from unwanted interference while enabling them to authorize interventions that they expect to advance their ends (so long as they are informed, free, and competent). In the context of the transaction at issue, it starts from the assumption that users have privacy rights over a substantial share of the personal data at issue in the transaction and that these rights would be infringed unless the SNS acquires valid consent. It thereby safeguards users' privacy-related interests in controlling their personal data, while enabling them to engage in freely chosen exchanges that they expect will serve their aims, so long as they have a good sense of what they might be getting into. It therefore claims to strike the right balance between what are often called the "protective" and "enabling" roles of consent (Miller and Wertheimer 2010; Dougherty 2020, 138). Moreover, the AA account can explain the qualms many have with existing notice-and-consent regimes, including in our opening Cambridge Analytica, Grindr, and Instagram cases. For, as we shall now detail, the consent mechanisms employed by SNS routinely fail to produce consent that fulfils the AA account's information, competence, and freedom conditions.

2.a Disclosure and understanding of information

The AA account requires that users be given substantial information by the SNS about how a particular exchange of personal data for access to services will change their rights of control over this data. They must also be given, or be able to readily access from other sources, information about the principal possible impacts of this exchange in terms of their key aims and values, along with a sense of the likelihood of these impacts. Failing to disclose this information may invalidate the user's consent because it unduly interferes with their decision-making process, thereby undermining the autonomy of their decision (Beauchamp 2010). As a result of such information provision, users must come to at least a rough understanding of the degree to which this transaction is likely to promote their aims. While the information appreciated by the user need not be complete, it needs to be sufficient for them to make a calculated gamble with a reasoned assessment of its up- and downsides, so that they have an opportunity to control what happens to them and the attainment of their ends (68).

Studies strongly suggest that these conditions are often not met in SNS-user interactions. First, privacy policies are often lengthy, the result being that users rarely read them (Custers et al. 2013; Schermer, Custers, and van der Hof 2014). They also change frequently, making it time consuming to stay abreast of the changes. The result is a high transaction cost for ongoing informed consent, leaving users unwilling to invest time in identifying the information relevant to their consent decision (Solove 2013; Joint Research Centre 2015). This leads to users being ill-informed about even the basic nature of the transaction. For example, studies find that most users falsely believe that

when a website has a privacy policy this means that this website cannot share personal data without their permission (Solove 2013, 1989; Acquisti, Brandimarte, and Loewenstein 2015, 512).

Second, there are limits to the extent to which the outcomes of data processing are predictable. With the fast-evolving power of modern data analytics, it is hard to predict what privacy-relevant information can be inferred from the personal data that users provide, and to which purposes this information may be put (Kosinski, Stilwell, and Graepel 2013). The risks also compound over time: the more personal information becomes available, the more predictive power algorithms have, and the more privacy-relevant information they may reveal (Hull 2015). It is therefore near impossible for a user to arrive at a reasoned assessment of the likelihood of possible implications of data processing when they consent to it (Solove 2013; Acquisti, Brandimarte, and Loewenstein 2015).

2.b Competence

Several factors threaten users' competence to make autonomous decisions concerning their personal data in the wide domain that the Privacy Self-Management paradigm allows. One aspect of such competence is simply the ability, when given access to relevant information, to arrive at a sufficient understanding of the pros and cons of a transaction (Feinberg 1986, chap. 26). But we have just seen that it is doubtful whether people generally possess this capacity in the context at hand.

Second, for users to be able to be self-directed in the sense of choosing in the light of their considered aims, they must have well thought-out, minimally stable preferences (Feinberg 1986, chap 26, sec. 1). Moreover, they must be able to ensure their choices are guided by these preferences rather than by factors that are irrelevant to what is at stake, such as the way a choice is framed (Hanna 2011, 528–29). However, research suggests that many people's preferences over the trade-off between limiting others' access to their personal data and gaining access to online services are ill-considered and unstable (Acquisti, Brandimarte, and Loewenstein 2015). Moreover, their choices are influenced by cognitive biases that are especially powerful in the context of the user-SNS transaction. These include the following.

Free Bias: Consumers underweight the nonmonetary costs of acquiring goods or services with a zero monetary price (Shampanier, Mazar, and Ariely 2007; Hoofnagel and Whittington 2014). As SNS typically set the monetary price of their service at zero, users will underweight the cost of granting SNS access to their data.

Present Bias: When considering a trade-off between well-being at time t and well-being at a later time, $t + n$, a present-biased person gives more weight to the well-being at t when t is the present than they do when making this trade-off at other moments (O'Donoghue and Rabin 1999, 103). Present bias is likely influential when it comes to making the cost-benefit analysis of joining an SNS, as the potential benefits often begin at once and are vividly presented, but the costs are less vivid and occur, if at all, at some future moment (Acquisti, Brandimarte, and Loewenstein 2015).

Default Bias: People tend to stick with default privacy settings out of convenience or due to an implicit belief that they are protective recommendations or "the norm." This bias is especially powerful in the user-SNS context, as there are often no stable, considered preferences to deviate from the default and few cues that are not under the control of the SNS (Solove 2013; Acquisti, Brandimarte, and Loewenstein 2015).

Finally, users' competence can be undermined by internal compulsion. While the extent of social media addiction is a matter of ongoing research (Zendle and Bowden-Jones 2019), there is evidence

that a substantial share of users engages with social media compulsively (and, by their own lights, excessively) and that part of the explanation for such behaviour lies in dopamine-mediated addiction (Lembke 2021).

2.c Free from controlling influences

Consent is free when it is not the result of coercion or manipulation. Due to the lack of understanding, the lack of stable, considered preferences, and the biases and self-control issues documented above, users' privacy choices on SNS are highly manipulable (Adjerid et al. 2013; Acquisti, Taylor, and Wagman 2016). Moreover, SNS have the knowledge and resources, as well as an incentive to exploit this manipulability to get users to reveal more information than they might wish (Acquisti, Brandimarte, and Loewenstein 2015; Warner 2019, 17–18). Indeed, exploiting users' decision-making foibles and potential for addiction is part of SNS' business model (Leslie 2016).

2.d The AA account's diagnosis of current problems with consent

Considering the surveyed factors inhibiting the autonomy of consent, on the AA account, currently common notice-and-consent regimes are inadequate. Appealing to these factors also allows the AA account to readily explain why relying on users' consent in our opening three cases is problematic. In the Cambridge Analytica and Grindr cases, the hiding of crucial information about extensive onward sale of personal data in lengthy, complex terms and conditions is a barrier to understanding, as was the fact that messages billed by Facebook as intended for a limited audience in fact were open to data processing and sale (Rosenblatt 2019). In the Instagram case, there is the further factor that information about the potential harmfulness of the service was not shared.

Several aspects of these cases also call into question users' competence. It is well-documented that Facebook has exploited default settings to get users to maximize the personal information that they share (Acquisti, Brandimarte, and Loewenstein 2015), and this practice also formed part of a complaint against Grindr (Norwegian Consumer Council 2018). In addition, some users' inability to control their time on Instagram was one of the findings of Facebook's research (Wells, Horwitz, and Seetharaman 2021). Since these forms of misrepresentation, failures of disclosure, and the exploitation of decision-making biases and lack of self-control were committed knowingly by firms intent on profit, these cases involve the exercise of controlling influence over users.

3. Against autonomous authorization as the basis for user-SNS exchange

One natural response to the analysis in section 2 is that consent regimes need to be reformed so that consent, when given, meets the AA account's standards. In what follows, we will argue against this response.

3.a Burdens

Our first objection is that measures to ensure users' autonomous authorization would impose barriers to access that are unduly burdensome and have inegalitarian impacts. Consider first that on the AA view, the SNS should provide the information that is likely to be relevant to the user's evaluation of the reasons they have for and against the transaction in a way that is readily comprehensible. Moreover, before proceeding, the SNS must have good reason to believe the user has arrived at a decent understanding of these pros and cons. For a wide variety of users, we submit that it is challenging to meet these conditions, even with supportive regulation. For reasons outlined in section 2, the possible ramifications of the provision of personal data are often extensive and complex, since it will not only determine the ads and content that a user is shown, but may also impact their personal relationships, reputation, job prospects, access to credit and insurance, and

risk of being exposed to discrimination, among others. Given the surprising inferences that can be drawn by sophisticated SNS or their clients on the basis of even small amounts of personal information, it is hard to explain, and grasp, the effects of providing access to individual pieces of data. Information that is sufficient to arrive at a reasoned assessment of the value of the transaction is therefore unlikely to be suitably succinct and easy to grasp to prompt users to master it. Regulators are aware of this problem, and some have attempted to limit the amount and complexity of information that users need to grasp by requiring users to provide granular consent for each purpose for which their data is processed rather than blanket consent to processing for a wide range of purposes (EU-GDPR.Info 2020.) However, this means that users are presented with an overwhelming amount of consent requests. These detract from the "low friction" online experience that they seek, and it is questionable whether users are thereby prompted to master the relevant material.

More radical steps would therefore be required to ensure that users understand the terms of exchange. SNS could, for example, be required to engage in questioning to establish whether a user understands the nature of the exchange to which consent is being sought and some of its key possible implications for their interests. The difficulty with such a proposal is that if the degree of understanding required were substantial enough for autonomous authorization, it would likely pose a significant barrier to access, which would also disproportionately block those with less education, "test-taking savvy," or digital nativeness from access to SNS. Individuals who would thereby be excluded may nonetheless reasonably judge that their engagement with SNS is instrumental to fulfilling their goals, even if they cannot fully grasp the nature of the exchange or its possible implications. Moreover, even individuals who could acquire the relevant understanding might reasonably object to the time and cognitive effort in doing so—especially since the fast-changing landscape would require frequent updates to their education. Indeed, the monetary equivalent of the time lost in merely reading the information contained in the privacy notices of all websites visited—let alone developing an appreciation of their significance—has been estimated at several thousand US dollars per year for the typical US adult (Acquisti, Brandimarte, and Loewenstein 2015, 513). We conclude that given the number of transactions involved, the complexity of the relevant information, the nebulousness of the potential consequences, and the need for people to prioritize their limited cognitive resources for other tasks, it is unreasonable to expect that the general public acquire a grasp of the stakes that is adequate for autonomous authorization.

Users' lack of considered preferences, the documented high degree of instability of the way people navigate the privacy-for-services trade-off, and the degree to which their choices are dependent on framing are likewise difficult to overcome. It would take extensive reflection on, and experience with, these novel trade-offs to generate more robust preferences. It is, of course, possible to challenge some framing effects. SNS could, for example, expose users to the same options framed differently and ask them to compare their choices in different frames and achieve consistency between them. But such an effort would be time-consuming and effortful. It may also be futile, since even the way choices are presented in this comparison (for example, their order) will have effects on people's final determinations, and psychologists note that often subjects are simply unable to resolve inconsistencies between their responses in different frames (Hanna 2011).

To hold that users' consent is not morally transformative for these reasons would prevent them from entering into transactions with SNS that they wish to engage in even when such transactions are, on balance, likely to advance their ends. Our first objection is, therefore that, given the considerable distance between the AA's standards and the circumstances of the general population, as well as the difficulties and costs of bridging this gap, the AA account does not adequately fulfil the "enabling" function of a theory of consent mentioned at the start of section 2.

3.b Power imbalances

Due to economies of scale in the provision of services and in extracting value from personal data, as well as network effects (the fact that the more users join an SNS, the more valuable it becomes to join it), markets in which SNS operate are highly concentrated and leading firms become entrenched (Haskel and Westlake 2018). This means that users have little choice between providers and that competition on the basis of the degree of privacy offered is limited. Moreover, in many countries, at least some SNS have become crucial to people's lives. This creates a stark power imbalance between users and SNS, as it is difficult to do without the services of a handful of key companies (Hill 2020). This allows SNS to restrict the value and range of options available to the parties they transact with (Leslie 2016). The Grindr case is an example: the company made access to its services conditional on accepting near unlimited onward sale of personal data. Because personal data only becomes valuable when aggregated (Hull 2015), individual users do not have leverage; users could only pose a threat to SNS by overcoming collective action problems and acting in unison to demand better terms, or by acting through governments.

The AA account claims that as long as the SNS' power is not used to coerce or manipulate, the range and quality of options they make available to users is not important for the latter's morally transformative consent (Beauchamp 2010, 72). Despite the importance of SNS' services in many people's lives, we take it that for many of the services where the terms on offer are objectionable, this is not because these terms are coercive. In our Grindr case, for example, the firm's stance that users gain access only if they agree to extensive onward sale of their data does not coerce users because forgoing Grindr's services would not have made them less well off than they have a right to be. In other words, these exchanges fail to meet one of the requirements for coercion, which is that the coercer threatens to make the party they are coercing worse off than a baseline to which the latter is morally entitled (Anderson 2021, sec. 2). For such noncoercive exchanges, the AA account registers neither the unfairness nor the loss in users' ability to pursue their interests that arise when (near) monopolies limit the options available to control users' personal data (see also Miller and Wertheimer 2010, 92 and 97). The account thereby overlooks the interest that users have in determining what is on the menu of privacy options. This is another sense in which the AA account does not adequately fulfil the "enabling" function of a theory of consent.

3.c Externalities

An individual's consent to data processing produces externalities. On the positive side, the consent of others who are like us makes it easier for firms to offer us goods and services that are tailored to our tastes. Other positive externalities include the potential to transform public-health surveillance by tracking geo-tagged flu symptom searches and mobility patterns in real time (Schmidt 2019). SNS also facilitate legitimate political action by enabling people to organise and mobilise, as was the case in the 2010 Arab Spring protests (Howard et al. 2011). On the negative side, others' sharing their data has implications for our privacy, since it enables firms to draw inferences about highly personal aspects of our lives even when we have shared only minimal information about ourselves. Though an individual may opt not to use an SNS, this does not prevent the SNS from gathering their personal data through the actions of their friends and acquaintances or monitoring them through their use of affiliated services. Effectively, this creates a society in which it becomes nearly impossible to opt out of the digital social network and maintain our privacy (Véliz 2020).

Finally, the concentration of economic, social, and political power in the hands of a few firms is problematic. An account which focuses only on bilateral consent transactions will miss the cumulative effects of these transactions on social arrangements and the concentration of power within society (Véliz 2020; Benn and Lazar 2022).

4. The value of choice account

We propose that, suitably adapted, T. M. Scanlon's (1998, chap. 6) Value of Choice theory can offer a better account of the permissibility of personal data processing by SNS. Scanlonian contractualism aims to find "principles that no one could reasonably reject" (249). The permissibility of conduct is determined by the reasons individuals have for wanting certain types of conduct to be permitted and the reasonable objections others might have to principles permitting such conduct (Kumar 2015). In deciding what one can reasonably reject, Scanlon holds that we must appeal not merely to how an individual ends up faring, but also to the value of the options they were given. He identifies three dimensions of such value: instrumental, representative, and symbolic. *Instrumental value* refers to the role of choice in securing what an individual has reason to want. For example, that a person has the choice about which degree to pursue is plausibly instrumental to their career satisfaction. An individual's choices may also be instrumental in allowing them to avoid harm, which we can refer to as the protective value of choice (Williams 2006). For example, if a person has a serious nut allergy, being offered a menu with detailed ingredients gives them the opportunity to avoid harm by choosing nut-free options. *Representative value* refers to the way in which a person's choices express their tastes and character, and *symbolic value* refers to the role of choice in signalling their competence and autonomy (Scanlon 1998, 251–53). For example, if the subject of a person's undergraduate degree was chosen by their parents, this may leave them alienated from their academic achievements and signal to others that they lack the competence to shape their life. When the opportunity to choose holds significant instrumental, representative, or symbolic value for a person, they have grounds to reject a principle denying them this opportunity.

In the context of the interaction between users and SNS, on the VoC view, autonomous consent is not the driving force of permissibility. Instead, what matters is that an individual has sufficiently valuable opportunities to achieve their aims and avoid harm (Scanlon 1998, 260–61). This requires a shift from attending merely to the person's knowledge, freedom, and competence at the moment of choice to attending to what—given their circumstances, dispositions, and abilities—they are likely to achieve by being offered a choice to trade access to personal data for access to services.

As long as the options are presented to users in ways that facilitate making the most of them, the opportunity to make choices regarding the processing of their personal data will have value of all three kinds for most individuals. There is positive instrumental value in developing our digital social network in a manner that reflects our aims. Choices concerning the disclosure of information are an important part of regulating our relationships and gradually deepening ties through the incremental disclosure of personal information (Rachels 1975). Such choices can also permit us to safeguard the other privacy-related interests outlined in section 1. The representative value of choices about our personal data is particularly relevant when considering our online identities. Having control over what is done with our data, who we share our data with, and what we share is essential for building an online identity that reflects who we are and how we wish to be perceived. Even the choice not to join a SNS can be an expression of values and character. Lastly, being given the power to make decisions about our personal data signals a recognition of our stake in the matter and of our standing to exercise control over it.

Scanlon (1998, 252) emphasizes, however, that these reasons "for valuing choice [are] both conditional and relative," in the sense that they depend on how well placed we are to use them to get what we have reason to want and to reflect aspects of ourselves. Naturally, they also depend on how the social context determines the symbolic value of choice. For example, decisions regarding the means of storing and transferring personal data securely may require such a level of technical expertise that asking a typical user to make them may lead to unsatisfactory outcomes, and therefore be of significant disutility and no protective value. The typical user could then not reasonably reject arrangements in which these choices were made for them by experts (as long as the latter were incentivized to make them in a manner that properly considered users' interests). Moreover, while withholding this choice may signal that the user is not competent to make this decision, this would

not be a slight, since most individuals are not well placed to make these choices and being recognized as well placed to do so is not an important sign of social status.

Naturally, people's ability to navigate a given set of options well is variable. However, in evaluating a set of options, Scanlon (1998, 205, 263) holds that we should simply consider which choices a *generic* user has reason to value and how such a generic user can be expected to fare given these opportunities. He does so because, he claims, it would be too demanding to take account of people's idiosyncrasies. We do not follow Scanlon's stance in this regard. For people's ability to make use of particular opportunities is significantly due to factors for which they are not fully responsible. It would therefore unfairly disadvantage those who have poorer, or atypical, choice-navigating abilities if we ignored these differences (Voorhoeve 2008). For example, there may be instrumental value for the generic user in having online advertising tailored to their personal tastes, interests, and behaviour since this may increase the efficiency of and satisfaction with purchasing decisions. They might also value having such targeting set as a default in order to save time and cognitive effort. However, consider the recovering alcoholic or gambler, who defaults into targeted advertising without the foresight that they are likely to receive advertising for liquor stores and casinos as a result (Acquisti, Taylor, and Wagman 2016), or the person who is insecure about their body and who does not realise that consent to targeted advertising means that two minutes of browsing on Instagram will lead to being exposed to a flood of ads for weight loss regimens featuring perfectly sculpted bodies (Wells, Horwitz, and Seetharaman 2021). Having to invest time and effort to avoid targeted advertising will not have positive value to such individuals, and in weighing reasons for and against a policy that permits it as a default, we should consider that it worsens the value of their opportunities in key respects.

We therefore propose that the value of a person's opportunity set should be determined by the (dis)value of the things they can achieve through their choices while taking into account how disposed they are to choose their better options and avoid their worse options (Voorhoeve 2008). In this evaluation, we should draw on research about how individuals' psychological traits and decision heuristics interact with the nature and presentation of options to affect the instrumental and representative value of choice. We thereby arrive at an account of the value of people's options that is suitable for diverse and boundedly rational individuals. This modification ensures that the account can capitalize on one aspect of the increasing use of personal data in the evolution of digital technologies, which is that the personalisation of online products and services offers an opportunity to tailor protective policies to highly disaggregated groups.

Two further aspects of the VoC view need highlighting. First, whether a person's opportunities are good enough (i.e., they could not reasonably reject facing these opportunities) is in part determined by what others would have to forgo in order to improve them. In the context of the user-SNS interaction, this means that we must assess how seriously SNS' legitimate interests (e.g., in profits from targeted advertising) would be set back if their users' opportunities were improved (e.g., by removing from the default settings a permission for unlimited sale of sensitive personal data). In this balancing of users' and SNS' interests, contractualists should, we submit, give greater weight to a given improvement in the interests of users precisely because they are less advantaged (Otsuka and Voorhoeve 2009, 183–84; *cf.* Scanlon 1998, 223–29).

Second, since it assesses moral rules by their suitability to serve as general principles of behaviour and social regulation, the contractualist approach outlined will consider the implications of the general availability of opportunities to trade access to personal data from the standpoint of other affected parties, such as fellow citizens. It thereby requires consideration of the cumulative social effects of such trades.

5. Why the value of choice avoids the problems with autonomous authorization

In order to grasp the similarities and differences between the AA and VoC accounts, it is useful to consider how they analyse our opening three cases. As we saw in section 3, the AA account focuses

on the failures of the SNS in these cases to meet conditions required for autonomous consent. The VoC account agrees that these exchanges are morally problematic but arrives at this verdict in a different way. On the VoC view, one key thing that is problematic in these cases is not the absence of autonomous consent but the fact that the opportunities that users faced were substantially less valuable than the SNS could readily have made them. We shall explain this difference between these approaches by considering in turn the information, competence, and freedom aspects of choice highlighted by the AA account, as well as concerns about power imbalances and society-wide interests.

5.a Presentation, disclosure, and understanding of information

In all three cases, users could reasonably have demanded more accurate, more extensive, or more usefully presented information. In the Cambridge Analytica case, one hindrance to users realising instrumental and representative value through their choices was that Facebook messages billed as "private" were, in fact, accessible to third parties. It would clearly be unreasonable for Facebook to reject the demand that it either change this misleading labelling or render such messages inaccessible to third parties. (Facebook has now done the latter [Wong 2018].) Moreover, in both the Cambridge Analytica and the Grindr cases, consent to extensive onward sale of sensitive personal data was hidden in lengthy and complex terms and conditions, which made it burdensome to come to know this important information and unlikely that users would, in fact, do so. Naturally, this is condemned by the AA account, which requires that information be provided in a manner that gives the recipient a decent opportunity to understand it (Millum and Bromwich 2018). Our version of the VoC account goes further by giving users a claim that the presentation of decision-relevant information is optimal, in the sense that this information will, in fact, "sink in" and prompt a wide variety of users to act in ways that are valuable to them given their diverse information-processing and decision-making abilities. Given many SNS' vast resources and knowledge, it is plausible that they can meet this claim at reasonable cost. If so, then there is a requirement for such widely useful information provision. In this respect, the VoC goes beyond the GDPR, which holds only that "the requirement that information is intelligible means that it should be understood by *an average member of the intended audience*" (Article 29 Working Party 2017, 7; emphasis added).

In the Instagram case, given that information about risks typically has protective value, the SNS could have improved users' opportunities by disclosing its internal research about these risks. While this disclosure might well have cost Facebook profitability, it is plausible that it was required because users have a stronger claim to be able to manage their exposure to such serious risks in this way than the company has to the profits it would forgo because of this disclosure. Here, the VoC account again aligns with the AA account. But the former appears to go further when we consider whether Facebook had an obligation to *conduct* this research on Instagram's effects on its users' mental health and to establish this research's findings with a greater degree of certainty (thereby obviating the company's defence that these findings were based on small sample sizes and so insufficient grounds for inferences about harm). For while the AA account includes a requirement that the party asking for consent know and disclose risks that are generally known in the field (Bromwich and Millum 2015), extant versions do not specify a duty for the agent seeking consent to use their powers to identify unknown risks of which they have an inkling. In contrast, on the VoC account, it is plausible that the SNS has an obligation to expend substantial resources to conduct research to fill in the data gaps on harms to users and ways in which these may be alleviated. For, on this account, users have a claim to the improved instrumental and representative value that this would enable them to achieve, and SNS are in a good position to meet this claim by virtue of being stewards of masses of behavioural data and having a unique capacity to analyse this data for users' benefit. Naturally, this obligation is circumscribed, since this interest of users must be balanced against SNS' interests. But, on a contractualist account that assigns due extra weight to the interests of the less advantaged, in the light of SNS' extraordinarily advantaged position, it is plausible that the upshot of

such balancing will require such fact finding. To put it differently, it is likely that users can reasonably reject a principle which absolves SNS from the duty to discover relevant harms. In this, the VoC aligns with commentators who argue that large SNS have such a duty (Zendle and Bowden-Jones 2019).

While in these respects, the VoC view may place more extensive demands on SNS than the AA account, it is important that in other respects it will be less demanding, especially of users' understanding. For the VoC account holds that it is not always necessary that there be stringent verification of users' understanding for their decision to access these services to be morally transformative. Opportunities to exchange data for access that are to a variety of users' advantage may be enough to render such processing permissible even if a user understands very little about the possible implications of the transaction or has simply ticked a box out of habit. Indeed, in cases where the background conditions for users are sufficiently favourable and the risks of harm small, it is likely that, on the VoC account, neither explicit consent nor substantial understanding of the nature of the exchange are necessary for the permissibility of data processing. In this sense, it aligns with one element of the EU GDPR, which specifies that merely by using services a person is taken to agree to the processing of data that is necessary for the provision of these services and for the "legitimate interests" of the service provider, so long as the data in question does not fall in a protected category (European Parliament and the Council of the European Union 2016, art. 6). The VoC account would add to the EU regulation, however, a requirement to consider whether the availability of the services in question on the terms involved is of sufficient value to a broad range of these services' users. The VoC account therefore gets these cases right without erecting excessive barriers to mutually beneficial exchanges.

5.b Competence and freedom

In all three of our cases, it is likely that a substantial share of users lacks well-considered preferences for balancing privacy against other goods. We also saw that SNS exploited users' decision-making biases in these cases, and that users in the Instagram case faced self-control problems. The AA account views these departures from standards of autonomous action as grounds for blocking the exchange of rights to process data for services. In contrast, the VoC focuses on the value of what users can achieve by being offered a choice given their abilities, biases, and dispositions. Naturally, a lack of determinate preferences represents a problem on the VoC account because it presents a barrier to some forms of representative value—a user can represent a definite picture of themselves and their values through their choices only when they know what they want—and to the assessment of options' instrumental value insofar as the latter is dependent on individuals' preferences. The lacunae in people's preferences may therefore require that the VoC account adopt a measure of the quality of people's options that is not wholly determined by their preferences, but also in part by general categories of interests (such as limiting who knows our HIV status or feeling confident about our body) and general conceptions of these interests' importance (see also Scanlon 2003). But these lacunae in people's preferences, their biases, and self-control problems do not, on the VoC account, always imply that exchanges between users and the SNS should be blocked. Instead of aiming for an ideal of informed, rational, well-considered choice, the VoC aims for what behavioural scientists refer to as a good "choice architecture" relating to the exchange of personal data (Thaler, Sunstein, and Balz 2012). It requires that SNS construct and present options so that a variety of users, with their limitations, can be expected to make choices that achieve their ends without undue risk of harm to themselves or others. On the VoC view, a key objection to SNS' actions in our three cases is that they failed to do so. Instead, they utilized users' biases or withheld information to maximize profits. By so manipulating users, SNS made it the case that users' choices reflected their weaknesses and the SNS' interests rather than users' values and aims. They thereby made users' opportunity sets significantly less valuable than they could reasonably have been made. For example, in the Grindr case, a change in default settings (to, say, a denial of permission to sell

data about HIV status) might well have substantially limited the risks users faced while leaving the company with ample scope to pursue profit. If this is so, then the VoC account would have required such a change. In the Instagram case, it is plausible that adjustments to Instagram's choice architecture and algorithms could lower the risks to users of encountering content that would exacerbate feelings of inadequacy without unduly disrupting the platform's financial model. Naturally, the precise type of action required will depend on facts about people's responses to various choice architectures. But the central point is that the VoC does not require that users overcome their cognitive and volitional shortcomings and become autonomous choosers before they can exchange access to data for services. Instead, taking users as they are, it requires that SNS structure the choice environment to users' advantage.

5.c Unequal power and external effects

All three cases exemplify the common situation in which users face a dominant firm that can set the terms of exchange and limit privacy options without much competitive pressure. We argued in section 3.c that on the AA account, this power asymmetry does not invalidate the exchange. By contrast, the VoC view is embedded in a contractualist view which grants the claims of the less advantaged extra weight. As outlined in sections 5.a and 5.b, the VoC view therefore requires that firms do not use their market power solely for their own advantage. It also requires policies that counteract this power asymmetry. One example is the measures taken in the EU to ensure that users can access basic services without giving permission to process sensitive personal data (unless such data is strictly necessary for service provision), thereby barring Grindr's demand for unlimited data processing as a condition for joining (European Parliament and the Council of the European Union 2016, art. 9; Norwegian Consumer Council 2018). It will also favour regulation of market structures to encourage competition and entry, so that users will have greater bargaining power when it comes to setting the terms of transactions and so that privacy protection is more likely to become a differentiator between providers. The VoC view should therefore prompt regulators to boost competition in the market, for example by prohibiting the common practice of takeovers of smaller firms by larger rivals.

Finally, where the AA account focuses only on the quality of consent in individual exchanges, the contractualist account that the VoC is part of considers the society-wide impact of principles of regulation for exchanges between users and SNS. It thereby offers a further route for criticism of the terms of exchange in some of our cases—most notably the Cambridge Analytica case, which highlighted the extent to which power to influence people's political views and actions has become dangerously concentrated. The view can therefore account for the fact that even exchanges that taken alone appear innocuous may cumulatively have unacceptable consequences. This ensures that it will rule out opportunities that are advantageous from the perspective the personal interests of individual users but which, if provided to all, would substantially worsen political and economic inequalities or rob those who choose not to engage with SNS of their privacy.

Conclusion

We have outlined the problem of consent that most SNS users are confronted with on a regular basis. Their personal data is used in ways they are unaware of and do not think they have agreed to, yet their consent forms the legal basis for the processing of their personal data. We have considered the view that the problem with existing consent mechanisms is that they fail to secure users' autonomous consent to the processing of their personal data and that these mechanisms should be reformed to secure such consent. We have argued that this view should be rejected for several reasons. First, the behavioral science of online activity shows that requiring autonomous consent would set the bar for access to SNS too high. Second, it does not sufficiently account for the power of SNS to set the terms of exchange. Third, it ignores the social effects of individual exchanges.

Drawing on T. M. Scanlon's contractualism and his views on the value of choice, we have offered an alternative theory that avoids these problems. On the proposed Value of Choice account, SNS gain permission to process users' personal data by providing users with sufficiently valuable opportunities to exchange access to personal data for services. We have argued that the value of these opportunities should be assessed for both (a) a wide variety of users given their cognitive limitations and decision-making abilities and (b) others who are affected by the general availability of these opportunities. A key policy implication is that regulatory regimes should shift their focus from obtaining autonomous consent to the use of personal data towards ensuring that users face options that they, with all their foibles, can be expected to use to advance individual and common interests.

Acknowledgements. Versions of this paper were presented at the Australian National University, KCL, the LSE, Universitat Pompeu Fabra, the University of Sydney, the US National Institutes of Health, and to the Society for Applied Philosophy. We thank those present and Matthew Adler, Seth Lazar, Adam Lovett, Joseph Millum, Bastian Steuwer, John Sweeney, an anonymous referee, and the editor of this journal for their comments.

Lichelle Wolmarans holds a BSc Hons in politics and philosophy from the London School of Economics and Political Science, through which she developed an interest in applied normative ethics relating to digital products and the data economy. She works as a user experience and service designer at PUBLIC, a technology company dedicated to public sector service innovation and transformation.

Alex Voorhoeve is professor in and head of the department of Philosophy, Logic and Scientific Method of the London School of Economics and Political Science. His research covers philosophy and public policy, decision theory, and moral psychology.

References

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. "Privacy and Human Behavior in the Information Age." *Science* 347 (6221): 184–97. https://doi.org/10.1126/science.aaa1465.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature* 54(2): 442–92. https://doi.org/10.1257/jel.54.2.442.

Adjerid, Idris, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2013. "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency." In SOUPS '13: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. https://doi.org/10.1145/2501604.2501613.

Anderson, Scott. 2021. "Coercion." In *The Stanford Encyclopedia of Philosophy* (Summer 2021), edited by Edward N. Zalta. https://plato.stanford.edu/archives/sum2021/entries/coercion/.

Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data. 2017. *Guidelines on Transparency under Regulation 2016/679*. 17/EN WP260. Accessed 12 January 2022. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

Barocas, Solon, and Helen Nissenbaum. 2014. "Big Data's End Run around Anonymity and Consent." In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum, 44–75. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781107590205.004.

Beauchamp, Tom L. 2010. "Autonomy and Consent." In *The Ethics of Consent: Theory and Practice*, edited by Frank Miller and Alan Wertheimer, 55–74. New York: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195335149.003.0003.

Beauchamp, Tom L., and James F. Childress. 2019. *Principles of Biomedical Ethics*. New York: Oxford University Press.

Benn, Claire, and Seth Lazar. 2022. "What's Wrong with Automated Influence?" *Canadian Journal of Philosophy*, First View: 1–24. https://doi.org/10.1017/can.2021.23.

Bowcott, Owen and Alex Hern. 2018. "Facebook and Cambridge Analytica Face Class Action Lawsuit," *The Guardian*, April 10, 2018. https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit.

Bowman, Courtney, and Kirsten Mathews. 2018. "The California Consumer Privacy Act of 2018." Proskauer (Privacy Law blog), July 13. https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

Bromwich, Danielle, and Joseph Millum. 2015. "Disclosure and Consent to Medical Research Participation." *Journal of Moral Philosophy* 12 (2): 195–219. https://doi.org/10.1163/17455243-4681027.

Custers, Bart, Simone van der Hof, Bart Schermer, Sandra Appleby-Arnold, and Noellie Brockdorf. 2013. "Informed Consent in Social Media Use—The Gap between User Expectations and EU Personal Data Protection Law." *Scripted* 10 (4): 435–57. https://doi.org/10.2966/scrip.100413.435.

Dougherty, Tom. 2020. "Informed Consent, Disclosure, and Understanding." *Philosophy & Public Affairs* 48 (2): 119–50. https://doi.org/10.1111/papa.12164.

Edenberg, Elizabeth, and Meg Leta Jones. 2019. "Analyzing the Legal Roots and Moral Core of Digital Consent." *New Media & Society* 21 (8): 1804–23. https://doi.org/10.1177/1461444819831321.

European Parliament and the Council of the European Union. 2016. "REGULATION (EU) 2016/679", *Official Journal of the European Community*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

EU-GDPR.Info. 2020. "Consent." Accessed December 4, 2020. https://gdpr-info.eu/issues/consent/.

Faden, Ruth R., and Tom L. Beauchamp. 1986. *History and Theory of Informed Consent*. New York: Oxford University Press.

Feinberg, Joel. 1986. *Harm to Self*. Vol. 3 of *The Moral Limits of the Criminal Law*. New York: Oxford University Press.

Gavison, Ruth. 1980. "Privacy and the Limits of Law." *The Yale Law Journal* 89 (3): 421–71.

Hanna, Jason. 2011. "Consent and the Problem of Framing Effects." *Ethical Theory and Moral Practice* 14 (5): 517–31. https://doi.org/10.1007/s10677-011-9266-y.

Haskel, Jonathan, and Stian Westlake. 2018. *Capitalism without Capital: The Rise of the Intangible Economy*. Princeton, NJ: Princeton University Press.

Hill, Kashmir. 2020. "I Tried to Live without the Tech Giants. It Was Impossible." *New York Times* July 31 2020. https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html.

Hoofnagel, Chris J., and Jan Whittington. 2014. "Free: Accounting for the Costs of the Internet's Most Popular Price." *UCLA Law Review* 61 (3): 606–70.

Howard, Philip N., Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari, and Marwa Maziad. 2011. "Opening Closed Regimes: What Was the Role of Social Media during the Arab Spring?" Working paper 2011.1. Accessed April 2021. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/117568/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_PITPI.pdf.

Hull, Gordon. 2015. "Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data." *Ethics and Information Technology* 17: 89–101. https://doi.org/10.1007/s10676-015-9363-z.

Joint Research Centre, Institute for Prospective Technological Studies, Shara Monteleone, Rene van Bavel, Nuria Rodríguez-Priego, and Gabriele Esposito. 2015. *Nudges to Privacy Behaviour: Exploring an Alternative Approach to Privacy Notices*. Publications Office. http://doi.org/10.2791/142795.

Kleinig, John. 2010. "The Nature of Consent." In *The Ethics of Consent: Theory and Practice*, edited by Franklin Miller and Alan Wertheimer, 3–22. New York: Oxford University Press.

Kosinski, Michal, David Stillwell, and Thore Graepel. 2013. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." *Proceedings of the National Academy of Sciences* 110 (15): 5802–5. https://doi.org/10.1073/pnas.1218772110.

Kumar, Rahul. 2015. "Contractualism and the Roots of Responsibility." In *The Nature of Moral Responsibility: New Essays*, edited by Randolph Clarke, Michael McKenna, and Angela M. Smith, 251–80. Oxford: Oxford University Press.

Lembke, Anna. 2021. *Dopamine Nation*. New York: Dutton.

Leslie, Ian. 2016. "The Scientists Who Make Apps Addictive." *1843 Magazine*, October 20, 2016. https://www.1843magazine.com/features/the-scientists-who-make-apps-addictive.

Miller, Franklin G., and Alan Wertheimer. 2010. "Preface to a Theory of Consent Transactions: Beyond Valid Consent." In *The Ethics of Consent: Theory and Practice*, edited by Franklin Miller and Alan Wertheimer, 79–105. New York: Oxford University Press.

Millum, Joseph, and Danielle Bromwich. 2018. "Understanding, Communication, and Consent." *Ergo* 5 (2). https://doi.org/10.3998/ergo.12405314.0005.002.

Norwegian Consumer Council. 2018. "Complaint against Grindr for Breaching Data Protection Law." Accessed April 26, 2020. https://fil.forbrukerradet.no/wp-content/uploads/2018/04/2018-04-03-complaint-grindr.pdf.

O'Donoghue, Ted, and Matthew Rabin. 1999. "Doing It Now or Later." *American Economic Review* 89 (1): 103–24. https://doi.org/10.1257/aer.89.1.103.

Otsuka, Michael, and Alex Voorhoeve. 2009. "Why It Matters That Some Are Worse Off Than Others: An Argument against the Priority View." *Philosophy & Public Affairs* 37: 171–99. https://doi.org/10.1111/j.1088-4963.2009.01154.x.

Rachels, James. 1975. "Why Privacy Is Important," *Philosophy & Public Affairs*, 4 (4): 323–33. https://www.jstor.org/stable/2265077.

Rosenblatt, Joel. 2019. "Judge: Facebook 'Could Not Be More Wrong' in Cambridge Analytica Defense.. *Insurance Journal*, September 11, 2019. https://www.insurancejournal.com/news/national/2019/09/11/539506.htm.

Scanlon, T. M. 1998. *What We Owe to Each Other*. Cambridge, MA: Harvard University Press.

Scanlon, T. M. 2003. "Value, Desire, and the Quality of Life." In *The Difficulty of Tolerance*, 169–86. Cambridge: Cambridge University Press.

Schermer, Bart W., Bart Custers, and Simone van der Hof. 2014. "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection." *Ethics and Information Technology* 16: 171–82. https://doi.org/10.1007/s10676-014-9343-8.

Schmidt, Charles. 2019. "Real-Time Flu Tracking." *Nature* 573: S58–59. https://doi.org/10.1038/d41586-019-02755-6.

Scism, Leslie. 2019. "New York Insurers Can Evaluate Your Social Media Use—If They Can Prove Why It's Needed." *The Wall Street Journal*, January 30. https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social-media-useif-they-can-prove-why-its-needed-11548856802.

Shampanier, Kristina, Nina Mazar, and Dan Ariely. 2007. "Zero as a Special Price: The True Value of Free Products." *Marketing Science* 26 (6): 742–57. https://doi.org/10.1287/mksc.1060.0254.

Singer, Natasha. 2018. "Grindr Sets Off Privacy Firestorm after Sharing Users' H.I.V.-Status Data." *New York Times*, April 3. https://www.nytimes.com/2018/04/03/technology/grindr-sets-off-privacy-firestorm-after-sharing-users-hiv-status-data.html.

Solove, Daniel J,. 2013. "Privacy Self-Management and The Consent Dilemma.' *Harvard Law Review* 126 (7): 1880–903.

Thaler, Richard, Cass Sunstein, and John Balz. 2012. "Choice Architecture." In *The Behavioral Foundation of Public Policy*, edited by Eldar Shafir, 428–39. Princeton, NJ: Princeton University Press.

Thomson, Judith Jarvis. 1990. *The Realm of Rights*. Cambridge, MA: Harvard University Press.

Vallor, Shannon. 2015. "Social Networking and Ethics." In *The Stanford Encyclopedia of Philosophy* (Winter 2016), edited by Edward N. Zalta. https://plato.stanford.edu/archives/win2016/entries/ethics-social-networking/.

Véliz, Carissa. 2020. *Privacy Is Power*. London: Penguin.

Voorhoeve, Alex. 2008. "Scanlon on Substantive Responsibility." *Journal of Political Philosophy* 16 (2): 184–200. https://doi.org/10.1111/j.1467-9760.2007.00297.x.

Warner, Mark R. 2019. *Potential Policy Proposals for Regulation of Social Media and Technology Firms.* White paper. https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.

Wells, Georgia, Jeff Horwitz, and Deepa Seetharaman. 2021. "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show." *Wall Street Journal,* September 14. https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

Williams, Andrew. 2006. "Liberty, Liability and Contractualism." In *Egalitarianism: New Essays on the Nature and Value of Equality*, edited by Nils Holtug and Kasper Lippert-Rasmussen, 241–61. Oxford: Oxford University Press.

Wong, Julia C. 2018. "Mark Zuckerberg Apologises for Facebook's 'Mistakes' over Cambridge Analytica." *The Guardian*, March 22. https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica.

Zendle, David, and Henrietta Bowden-Jones. 2019. "Is Excessive Use of Social Media an Addiction?" *BMJ* 365 (2171). https://doi.org/10.1136/bmj.l2171.

Cite this article: Wolmarans, L. and Voorhoeve, A. 2022. What Makes Personal Data Processing by Social Networking Services Permissible? *Canadian Journal of Philosophy*: 1–16, doi:10.1017/can.2022.4