JCP JOURNAL OF CONSUMER PSYCHOLOGY

SCP SOCIETY FOR CONSUMER PSYCHOLOGY

This article is part of a Research Dialogue:
Krishna (2020): https://doi.org/10.1002/jcpy.1186
Acquisti et al. (2020): https://doi.org/10.1002/jcpy.1191
Mulligan et al. (2020): https://doi.org/10.1002/jcpy.1190
Jagadish (2020): https://doi.org/10.1002/jcpy.1188
Acquisti et al. (2020): https://doi.org/10.1002/jcpy.1187

Identity-Based Motivation and the Logic of Conversations Obfuscate Loss of Online Privacy and What Policy-Makers Can Do About It

Daphna Oyserman, and Norbert Schwarz
University of Southern California

Accepted by Associate Editor, Aradhna Krishna

People care about their privacy, but when they are online, they do not act as if they do. We apply the psychology of meaning-making to shed light on why that is. Acquisti, Loewenstein, and Brandimarte (2020) review of factors relevant to gaps between privacy attitudes and behaviors highlights both the importance of the problem of online privacy and its intractability, given current thinking about what can be done. Connecting their discussion with the psychology of meaning-making, operationalized by integrating identity-based motivation theory with the logic of communication and anthropomorphizing, this commentary addresses why people narrowly conceptualize what privacy they are losing and fail to act as if privacy matters, as well as what can be done about it at a policy level.

Keywords Cognition; Communication; Economic psychology; Meta-cognition and metacognitive experience; Online consumer behavior; Product and product design; Public policy issues; Self and identity

People have relationships with their personal electronic devices and online applications and find them to be part of who they are. Their devices and user-interfaces invite personalization and users engage conversationally with their "talking map", their Apple Siri or Google assistant as they would with individuals. Deeply built into the experience is the idea of personalized goal pursuit, doing things in your own way, to get exactly what you want by engaging in a conversation. As part of this conversation, people share some information (e.g., location tracking) for the purpose of gaining knowledge relevant to pursuing their goals (e.g., nearby places serving Thai food, how to get to the conference center). In real life, when asking for directions from another person, people do not assume that the person they are asking has been waiting at the street corner hoping to ensnare them in an information seeking venture. Instead, they infer that the other is simply a cooperative by-stander, willing to help if they receive the relevant information. Similarly, in sharing online, people fail to recognize that they are the product. Instead, they assume that they are engaging with the platform to attain their own goals. They assume the platform is incidental, like a human passerby. Because of this, they may assume that when they give some information, the rest of their personal information is not accessed. After all, if I ask you for directions, you need to know where I am now and where I trying to go—but that neither means you will always know where I am, nor that you will also know which news sites I visit. It surely does not follow that you will sell all of that to others.

Received 23 July 2020; accepted 2 August 2020
Available online 06 September 2020
Correspondence concerning this article should be addressed to Daphna Oyserman, Department of Psychology, University of Southern California, Los Angeles, CA 90089-1061, USA. Electronic mail may be sent to oyserman@usc.edu.

 1057-7408/2020/1532-7663/30(4)/759–766
DOI: 10.1002/jcpy.1189

Apps, social media, and search engine sites benefit when people experience them as friendly tools or parts of their identities and actively seek to trigger anthropomorphizing and identity by imbuing interactions with personalizing and interpersonal touches. Thinking about applications as friends and using them as part of being a savvy person who can get what they want obscures privacy as a concern. Like a friend who knows what you like and can finish your thoughts, your apps are there for you; they help you be yourself, being yourself entails tailoring, that requires sharing. Identity-based, anthropomorphizing frames yield the odd observation that Acquisti, Loewenstein, and Brandimarte (2020) highlight, which is that people care about their privacy, but when they are online, they do not act as if they do.

As Acquisti, Loewenstein, and Brandimarte emphasize, unless something changes, it is unlikely that privacy will be regained. Individual actors cannot negotiate their privacy with institutional actors and regulators are frequently coopted by the industries they are meant to reign in. In our commentary, we draw on the psychology of meaning-making to outline how privacy concerns are obfuscated in online interaction, highlighting how online interactions are set up to turn on people's identity-based motivation using the logic of communication and anthropomorphizing. We suggest that people misinterpret their online interactions as being about expressing their identities with the assistance of applications in part because they see these interactions as analogous to interactions with humans and this narrows their privacy concerns. To keep privacy concern narrowly focused and reduce sense of control over personal information, institutional actors use personalizing and anthropomorphizing techniques to increase a feeling of identity expressiveness and sociability. They position and formulate privacy policies in ways that make it difficult for people to determine what they are sharing with whom and what they can do about it. We conclude with a discussion of what can be done to increase the odds that people see the scope of privacy loss and engage in effective action to protect their own privacy.

Identity-Based Motivation: Thinking (About The Self) Is For Doing

As William James (1890) emphasized, thinking is for doing. People go online for a purpose (expressing themselves, working, shopping, being informed or entertained). Online as well as offline, most goal pursuit requires some disclosure of information or else the goal will not be achieved. In marketplace interactions, disclosure is legitimized by its functionality, from sharing product preferences to sharing payment information or one's GPS position while searching for a restaurant. Sharing is often framed as ways to tailor, yield an outcome that fits who one is or wants to become, increasing the likelihood that people will experience their online activities as identity-congruent, something that they and people like them do to attain their goals. When an action feels identity-relevant, any impediments along the way will feel like obstacles to be overcome, not signals that the action or the goal itself should be dropped.

In writing this piece, one of us asked Google for the "percentage of people using the internet". The top-ranked response came from a site which informed me that by proceeding, I was accepting their use of cookies. A green button suggested I click OKAY. Small print informed me that if I wanted to learn more about their policies, I could click F1. So, I did. Nothing happened. What to do? Drop the information search goal? That was the moment in which privacy concerns could have been triggered. That agreeing was made easy (press a big button or simply continue), whereas disagreeing was made difficult (pressing F1 yields no results), is a design feature, not a flaw. Some platforms direct people to email to obtain information regarding which information is tracked and how it is used, with the implication that the choice is agree and use now, or disagree, and find a different route to goal attainment.

Given that online interactions are self-initiated, people may feel that the action is identity-congruent, fits with who they are and are trying to become (Oyserman, 2009a, 2009b; Oyserman, Destin, & Novin, 2015). Once an aspect of identity is on-the-mind, it shapes how people make sense of their opportunities and experiences (Oyserman, 2007; Oyserman, Elmore, & Smith, 2012). People vary in which aspect of identity is triggered by online engagement. For some, online engagement implies that they are savvy, the kind of people who can cleverly use the latest tools to get what they want. For others, it implies that they are astute, getting information from the source rather than filtered. Rarely do people go online in order to show themselves that they are good stewards of their personal information. Privacy rarely becomes focal because it is not what people are trying to do online. On-the-mind goals increase the accessibility of goal-related information and impair the accessibility of

competing (or irrelevant) information (Bruner, 1957; Fishbach & Ferguson, 2007).

When privacy does come to mind, it is usually after information that seems relevant to the personal goal has been disclosed. Indeed, online platforms frame information requests as ways to provide personally tailored goods and services, making sharing feel like a self-focused activity (e.g. "what do I really want?"). Hence, people are most likely to consider privacy issues when they reach the stage of providing payment information. Yet, whether people pay or not, they have already engaged in a long sequence of goal-related information sharing. This sequencing focuses consumers on one aspect of privacy, "identity theft" and its possible credit implications. What people miss is that the mere initiation of an online interaction is the beginning of information disclosure. People are typically unaware that in providing any information (what they are looking for, worried about, enjoy and prefer), they have agreed to have the online platform use it, bundle it, and sell it to others. Privacy concerns that are focused on identity theft can be allayed through safe-payment mechanisms, "trusted site" badges and identity monitoring services. Notably, each of these provides profitable business opportunities for industry, while focusing consumers on aspects of privacy that pose little threat to the interests of commercial and political online actors interested in user data.

Monetizing information gathered online is big business. Almost all (9 in 10) Americans are online, some accessing the internet only through social media or other smartphone applications (Pew Research Center, 2019). Not everyone who uses the internet sees themselves as internet users, those who engage directly with smartphone applications and social media often do not (Pew Research Center, 2019). This misunderstanding likely decreases people's sense that privacy is an issue. They mostly think of their sharing as limited to friends and existing in the moment (ephemeral) rather than as permanently captured and bundled for commercialization. As in personal interactions, people typically do not consider privacy in making social media posts—that I enjoyed dinner at Little Sister, that I visited the pier with my daughter and granddaughters, that I read the Washington Post, none of this seems worth hiding. Framing privacy itself as having something to hide implies that what is being hidden is either something to be embarrassed about or something that could be costly if revealed.

What people miss is that monetizing information is not just about embarrassing secrets or obtaining credit card information. The broader issue of online tracking and information linkage across many activities is for the purpose of delivering finely tuned persuasive messages. Messaging can take the form of targeted commercial (Johnson, 2013) and political (Bradshaw & Howard, 2018) advertisements and infomercials. Beyond targeting by prior site visits, persuasion attempts are framed in ways that feel fluent, fit cultural scripts and are personalized to feel identity-congruent (Oyserman, 2019a, 2019b; Oyserman & Dawson, 2020). Campaigns can craft messages, not with the goal of informing but with the goal of changing action regardless of the truth value of the message (Oyserman & Dawson, 2020). The latter version of persuasion involves using my posts, and everything else about my online presence, and geocoding, to link up to a wealth of information about who I am, what sorts of things matter to me, and hence, what concrete frames, images, and tag lines might sway me. My posts link me to a web of others all of whom can be targeted not simply to advertise the latest Asian-French fusion but also to frame persuasive attempts. Disinformation is information presented without regard for truth value, with the goal of triggering action. Disinformation works best when linked to images and taglines that feel fluent because they are relevant to my own identities and because they follow cultural scripts. What feels fluent to me, what fits my identities and cultural scripts, can all be gleaned through synthesizing everything about myself that I have provided online free for use. A clear example outside the United States entails the U.K. referendum on whether to stay or leave the E.U. (Oyserman & Dawson, 2020). While the groups working to remain in the E.U. used factually correct targeted information campaigns highlighting concerns relevant to each targeted voter group (e.g., about the economy, about treaties), the groups working to leave the E.U. employed disinformation.

A scathing report from the U.K. Parliament (2019) likened Facebook executives to "digital gangsters" for their handling of user data and highlighted Facebook's role in providing the raw materials for Cambridge Analytica to develop and disseminate via Facebook and other social media platforms images and taglines that were dis-informative—developed without regard for truth value with the goal of getting voters who thought Britain should stay in the E.U. to stay home rather than vote while mobilizing voters who thought Britain should leave the E.U. People likely to vote to remain in the E.U. were treated to images implying corruption and regulations harming ecological

concerns, including harming polar bears. These confusing images served the goal of sowing confusion as to whether staying was really the right thing to do. Left in doubt, young people who favored staying, failed to vote. In contrast, older voters were served with images of red double decker buses and warnings that the EU would steal your "cuppa" (culturally fluent description of a cup of tea). These worried voters voted *en masse* to leave. None of these voters had knowingly provided the raw materials for these successful persuasions. They thought they were sharing innocuous posts about their meals, their granddaughters, their local beach, their opinions. But knowing who I am (have granddaughters, live in a mostly white place, with mostly wealthy neighbors) and what I like (the news I share) provides the grist for the disinformation mill.

Our mental models of interacting with shop keepers and friends, our ways of showing one another who we are, documenting our tastes and desires, do not include the possibility that where we have been, what we have said, where we have clicked, will be bundled and sold to unknown others, to use in combination with data analytics to fill in gaps with knowledge gained from similar others to design tailored influence attempts. This scenario is far removed from self-disclosure and privacy protection in personal interactions (cf. Altman, Vinsel, & Brown, 1981). It is also not closely linked to the sequence of behaviors involved in most goal-directed online interactions. Indeed, except for fringe actors endorsing political conspiracy theories (Samory & Mitra, 2018) and dissidents in authoritarian regimes (Hahn & Layne-Farrar, 2002) there are few noncriminal online activities where the core goal of the activity is likely to bring large-scale information tracking and pooling to mind.

Communication is Cooperative

Consumers not only accept that they need to disclose information that is clearly required for the ongoing interaction, they are also unlikely to question the legitimacy of tangential information requests as part of an ongoing exchange. This reflects, in part, that people bring the tacit assumptions that govern communication in everyday life (Grice, 1975) to the online context. They assume that speakers provide information that is relevant to the goal of the exchange, truthful and clear, and that speakers expect such information in return (Grice, 1975; Schwarz, 1994; Sperber & Wilson, 1995). This is at the heart of many context effects in judgment and decision making, including consumers' reliance on the frames of reference conveyed by the response alternatives provided in questionnaires (Schwarz, 1994, 1995) and online forms (Hauser & Schwarz, 2019). These tacit assumptions also seem to guide consumers' processing of privacy information, leading them to proceed as if all relevant information was provided in the short and readable summary and to ignore the indigestible legalese (which surely would have been explained in a more accessible way if it really were important).

People only suspend the assumptions of cooperative conversational conduct when they see reasons to distrust the communicator (Mayo, 2015; Schwarz, 1996; Schwarz & Lee, 2019) or have reason to believe that the communicator is not human (Lin, Zhang, & Oyserman, 2020). Service platforms and online companies work hard to avoid both inferences, supported by a plethora of personalizing and anthropomorphizing techniques and "trusted site" designations. Hence, consumers are likely to operate within the constraints of the limited choices offered to them and accept vaguely formulated privacy policies that allow firms to collect, use, and share their personal information with other organizations. This sharing allows the construction of an increasingly detailed profile of who they are and what they do, which can be used to sell them products at prices tailored to their financial ability or to influence their attitudes or voting behavior.

One of the most efficient and cost-effective interventions would be regulations that require sites to unpack their privacy policies and to ask for separate, explicit permissions for each of these components. As Acquisti et al. (2020) pessimistic discussion of regulatory efforts indicates, such regulations would face considerable opposition because selling information and access is lucrative and central to the business models of large social platforms.

Online Interactions are Anthropomorphized

One reason that people fail to notice that privacy is broader than the sharing of their credit card information is that they reason about privacy in online interactions as if they were having a personal interaction with another human. That is, they interact with online agents (their map site, their restaurant guide, their browser) as if they were interacting

with a person. Because they anthropomorphize their online interaction partners, they attribute human attributes to them—they are helpful, friendly, patient, knowledgeable, reliable, trusted. In the interpersonal domain, disclosure is usually limited to the persons present during the interaction and while indiscretions can happen, the risk is mutual and limited by reputational concerns (Altman et al., 1981). Not so online, where disclosure is asymmetrical and the disclosed information sold and pooled across many disclosures, each of which was made to a different, and usually anonymous, agent. Once bundled, analyzed and complemented by analytic insights, the shared information is more than people think they have shared with any online site.

Companies, service platforms, and hardware providers encourage anthropomorphizing in numerous ways, from chat bots to virtual assistants with human voices and natural language comprehension (Nass & Brave, 2005; Rauschnabel & Ahuvia, 2014). Not too long ago, it was an amusing oddity when people gave their computer a name, pleaded with it when slowed or reciprocated its good behavior (Reeves & Nass, 1996); now, talking with Siri, Alexa and their sibs is a familiar part of life. This has consequences. Experimental research indicates that the perceived trustworthiness and competence of nonhuman agents increases with their anthropomorphization and the more people anthropomorphize nonhuman agents, the more they accept the agents' choices and requests (Gong, 2008; Kim & Sundar, 2012; Nass & Brave, 2005; Pak, Fink, Price, Bass, & Sturre, 2012). Companies are aware that people are more willing to reveal extra information in anthropomorphized interchanges (Thomaz, Salge, Karahanna, & Hulland, 2020) and make efforts to anthropomorphize themselves, their brands, and specific products (Aggarwal & McGill, 2007; Chandler & Schwarz, 2010; Kniazeva & Belk, 2010; Podnar & Melewar, 2010; Stinnett, Hardy, & Waters, 2013).

We suspect that when people anthropomorphize their online interaction, they are more likely to think in terms of interpersonal privacy and less likely to notice or consider institutionalized pooling of information across many interactions. This suggests that consumers will be more worried about prototypical interpersonal privacy concerns while talking with Alexa, Siri or the Google Assistant than when doing a keyboard-based search, whereas the opposite should hold for privacy concerns related to institutional data capture and sharing. What people miss is that no matter the interface, data capturing, pooling, bunding, and selling are always critical to the business model.

Important or Impossible? Identity-Based Motivation

Everyone has had the experience of trying to understand what exactly they are agreeing to when reading a privacy policy, only to eventually give up and decide that it is impossible to understand and not really worth their time to try. This gut-based response reflects a close association of difficulty and impossibility in the English language (Yan & Oyserman, 2020) that can also be captured with implicit measures (O'Donnell & Oyserman, 2020). When led to interpret difficulty as impossibility, people become unsure if a task is identity-relevant, undermining their willingness to engage (Aelenei, Lewis, & Oyserman, 2017; Oyserman, Elmore, Novin, Fisher, & Smith, 2018; Smith & Oyserman, 2015). People are likely to interpret difficulty as a sign of impossibility when they are unsure about which aspect of their identity is relevant in a situation (Oyserman, Bybee, & Terry, 2006; Oyserman et al., 2015). When they are sure a task or situation is relevant to their identities, they interpret difficulty as evidence that the task is important and valuable to them (for a review, see Oyserman et al., 2017). Not surprisingly, perceived importance motivates engagement, whereas perceived impossibility impairs it.

This has implications for privacy protection. The identities that are on consumers' minds when they encounter a privacy policy are related to the goals that brought them online in the first place—connecting with friends, finding the perfect dress, or supporting one's argument in a JCP commentary with a good reference. In the moment of pursuit, failing to pause to figure out how to disable invasive tracking (if that is even possible) is likely, and in retrospect, this failure implies that one probably is not worried. Moreover, as noted above, privacy is rarely one's primary goal. When privacy concerns come to mind, they are often dominated by worries about theft of credit card, banking, or social security numbers, and the need to protect these from malicious actors who want to sell them on the "dark" web. If one only shares this kind of information with actors one trusts enough to do business with, and they are not hacked by thieves, terrible outcomes are not expected. If online privacy about as "theft" and the "dark" web, then wanting to

"hide" online behavior from view may feel at odds with the self-perception that one has "nothing to hide". Hence, consumers' most common protective behaviors are limited to what their banks recommend—protecting passwords, using anti-virus software, and being cautious with public wi-fi.

Overcoming the numerous hurdles imposed by privacy policies requires attention, persistence, and the acquisition of relevant skills. To motivate this engagement, people must see privacy protection not only as relevant to their goals, but also as identity-congruent—something that "people like me" do. Ironically, privacy protection is itself a rather private behavior and rarely the topic of personal discussion. This impairs the development of descriptive norms regarding these behaviors (Cialdini, 2003) that could convey that engaging in identity protection is a common activity for "people like me" (Oyserman, 2007). Finally, whether people perceive a challenging task as worth their while also depends on how much control they have over it. As Mourey and Waldman (2020) observed, people perceive privacy as less important when a company or their social network manages it, than when they themselves manage it, especially when privacy management is difficult.

Next Steps

So, what can be done? First, public information campaigns need to clarify what online transactions entail—no matter how personable the app, online transactions are not interactions with friendly others, they are not merely ways of expressing yourself. As the saying goes, "If you're not paying for it, you are the product." In fact, you are the product even if you do pay because collecting and bundling information, filling in the gaps with analytics, and selling the results is big business that companies protect with difficult-to-parse terms of use and privacy information, as Acquisti et al. (2020) review. Hence, the appropriate interpretation of experiences of difficulty should not be "this is impossible for me, my time is better spent elsewhere." But rather, "this experience of difficulty is a signal of how important it is *for them* to get me to agree."

Public information campaigns need to emphasize that the information people freely provide in one "interaction" and with one interaction "partner" streams from their phones and web-browsers continuously and not only for the specific user-instigated purpose or interaction. That this information is bundled and analyzed in connection with information provided in other "interactions" for other purposes, synthesized, and used for purposes that people did not intend or agree to (e.g., persuasion attempts tailored in ways that will feel identity-congruent and culturally fluent and hence not carefully scrutinized).

Because information becomes more valuable, and privacy more impinged, the more continuously information is collected and the more it is linked to other information, consumers need to know for how long and for what purposes their information is used. There is no reason that companies should leverage people's identity-based motivation and understanding of the logic of communication against them. Instead, public regulators can use both to formulate privacy policy and consent, including explicit opt-in procedures for different types of information and different uses of that information. Much like research in other domains is regulated by human subject policies, overseen by review boards, and linked to explicit consent, online data collection, storage, and use through companies requires regulation and consent—it is, after all, human subject research. Just because companies benefit from bundling and selling consumer profiles, does not mean that consumers need to be forced to agree to it, especially given that profiling is used to shape consumer attitudes, judgments, and behaviors. Change will be difficult to achieve because it goes against influential interests—but here as elsewhere, difficulty signals importance, not impossibility.

References

Acquisti, A., Loewenstein, G. & Brandimarte, L. (2020). Privacy lost/privacy refound. *Journal of Consumer Psychology*.

Aelenei, C., Lewis, N. Jr, & Oyserman, D. (2017). No pain no gain? Social demographic correlates and identity consequences of interpreting experienced difficulty as importance. *Contemporary Educational Psychology*, *48*, 43–55. https://doi.org/10.1016/j.cedpsych.2016.08.004

Aggarwal, P., & McGill, A. L. (2007). Is that car smiling at me? Schema congruity as a basis for evaluating anthropomorphized products. *Journal of Consumer Research*, *34*, 468–479. https://doi.org/10.1086/518544

Altman, I., Vinsel, A., & Brown, B. B. (1981). Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. *Advances in Experimental Social Psychology*, *14*, 107–160.

Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: A global inventory of organized social media

manipulation. *The Computational Propaganda Project*, *1*. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Bruner, J. S. (1957). On perceptual readiness. *Psychological Review*, *64*, 123–152. https://doi.org/10.1037/h0043805

Chandler, J., & Schwarz, N. (2010). Use does not wear ragged the fabric of friendship: Thinking of objects as alive makes people less willing to replace them. *Journal of Consumer Psychology*, *20*, 138–145. https://doi.org/10.1016/j.jcps.2009.12.008

Cialdini, R. B. (2003). Crafting normative messages to protect the environment. *Current Directions in Psychological Science*, *12*, 105–109. https://doi.org/10.1111/1467-8721.01242

Fishbach, A., & Ferguson, M. J. (2007). The goal construct in social psychology. In A. W. Kruglanski, & E. T. Higgins (Eds.), *Social psychology: Handbook of basic processes* (2nd edn, pp. 490–515). New York, NY: Guilford Press.

Gong, L. (2008). How social is social responses to computers? The function of the degree of anthropomorphism in computer representations. *Computers in Human Behavior*, *24*, 1494–1509. https://doi.org/10.1016/j.chb.2007.05.007

Grice, H. P. (1975). Logic and conversation. In P. Cole, & J. L. Morgan (Eds.), *Syntax and semantics, Vol. 3: Speech acts* (pp. 41–58), New York, NY: Academic Press.

Hahn, R. W., & Layne-Farrar, A. (2002). The benefits and costs of online privacy legislation. *Administrative Law Review*, *54*, 85–172.

Hauser, R., & Schwarz, N. (2019). Score blending: How scale response grouping biases perceived standing. *Journal of Behavioral Decision Making*, *32*, 194–202. https://doi.org/10.1002/bdm.2107

James, W. (1890). *Principles of psychology*. New York, NY: Henry Holt.

Johnson, J. P. (2013). Targeted advertising and advertising avoidance. *The RAND Journal of Economics*, *44*, 128–144. https://doi.org/10.1111/1756-2171.12014

Kim, Y., & Sundar, S. S. (2012). Anthropomorphism of computers: Is it mindful or mindless? *Computers in Human Behavior*, *28*, 241–2500. https://doi.org/10.1016/j.chb.2011.09.006

Kniazeva, M., & Belk, R. W. (2010). If this brand were a person, or anthropomorphism of brands through packaging stories. *Journal of Global Academy of Marketing*, *20*, 231–238. https://doi.org/10.1080/12297119.2010.9707349

Lin, Y., Zhang, C., & Oyserman, D. (2020). Seeing meaning even when none exists: Collectivism increases belief in empty claims. Manuscript under editorial review.

Mayo, R. (2015). Cognition is a matter of trust: Distrust tunes cognitive processes. *European Review of Social Psychology*, *26*, 283–327. https://doi.org/10.1080/10463283.2015.1117249

Mourey, J. A., & Waldman, A. E. (2020). Past the privacy paradox: The importance of privacy changes as a function of control and complexity. *Journal of the Association for Consumer Research*, *5*, 162–180. https://doi.org/10.1086/708034

Nass, C. I., & Brave, S. (2005). *Wired for speech: How voice activates and advances the human-computer relationship*. Cambridge, MA: MIT Press.

O'Donnell, S. C., & Oyserman, D. (2020). *Do social networks reflect shared interpretations of difficulty?* Unpublished manuscript. Los Angeles, CA: University of Southern California.

Oyserman, D. (2007). Social identity and self-regulation. In A. Kruglanski, & T. Higgins (Eds.), *Handbook of social psychology* (2nd edn, pp. 432–453). New York, NY: Guilford Press.

Oyserman, D. (2009a). Identity-based motivation: Implications for action-readiness, procedural readiness, and consumer behavior. *Journal of Consumer Psychology*, *19*, 250–260. https://doi.org/10.1016/j.jcps.2009.05.008

Oyserman, D. (2009b). Identity-based motivation and consumer behavior. *Journal of Consumer Psychology*, *19*, 276–279. https://doi.org/10.1016/j.jcps.2009.06.001

Oyserman, D. (2019a). The essentialized self: Implications for motivation and self-regulation. *Journal of Consumer Psychology*, *29*, 336–343. https://doi.org/10.1002/jcpy.1093

Oyserman, D. (2019b). Cultural fluency, mindlessness, and gullibility. In R. Baumeister, & J. Forgas (Eds.), *The social psychology of gullibility: conspiracy theories, fake news and irrational beliefs* (pp. 255–278). New York, NY: Routledge/Psychology Press.

Oyserman, D., Bybee, D., & Terry, K. (2006). Possible selves and academic outcomes: How and when possible selves impel action. *Journal of Personality and Social Psychology*, *91*, 188–204. https://doi.org/10.1037/0022-3514.91.1.188

Oyserman, D., & Dawson, A. (2020). Your fake news, our facts: Identity-based motivation shapes what we believe, share, and accept. In R. Greifeneder, M. Jaffé, E. J. Newman, & N. Schwarz (Eds.), *The psychology of fake news: Accepting, sharing, and correcting misinformation*, (173–195). London: Psychology Press.

Oyserman, D., Destin, M., & Novin, S. (2015). The context-sensitive future self: Possible selves motivate in context, not otherwise. *Self and Identity*, *14*, 173–188. https://doi.org/10.1080/15298868.2014.965733

Oyserman, D., Elmore, K., Novin, S., Fisher, O., & Smith, G. (2018). Guiding people to interpret their experienced difficulty as importance highlights their academic possibilities and improves their academic performance. *Frontiers in Psychology*, *9*, article 781. https://doi.org/10.3389/fpsyg.2018.00781

Oyserman, D., Elmore, K., & Smith, G. (2012). Self, self-concept, and identity. In M. R. Leary, & J. P. Tangney (Eds.), *Handbook of self and identity* (pp. 69–104). New York, NY: The Guilford Press.

Oyserman, D., Lewis, N. A. Jr, Yan, V. X., Fisher, O., O'Donnell, S. C., & Horowitz, E. (2017). An identity-based motivation framework for self-regulation. *Psychological Inquiry*, *28*, 139–147. https://doi.org/10.1080/1047840X.2017.1337406

Pak, R., Fink, N., Price, M., Bass, B., & Sturre, L. (2012). Decision support aids with anthropomorphic

characteristics influence trust and performance in younger and older adults. *Ergonomics*, *55*, 1059–1072. https://doi.org/10.1080/00140139.2012.691554

Pew Research Center (2019). https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

Podnar, K., & Melewar, T. C. (2010). Understanding and interpreting the relationship between human and corporate identity: An empirical study. *Global Business and Management Research: An International Journal*, *2*, 366–385.

Rauschnabel, P. A., & Ahuvia, A. C. (2014). You're so lovable: Anthropomorphism and brand love. *Journal of Brand Management*, *21*, 372–395. https://doi.org/10.1057/bm.2014.14

Reeves, B., & Nass, C. I. (1996). *The media equation: How people treat computers, television, and new media like real people and places*. New York, NY: Cambridge University Press.

Samory, M., & Mitra, T. (2018). The government spies using our webcams. *Proceedings of the ACM on Human-Computer Interaction*, *2*, 1–24. https://doi.org/10.1145/3274421

Schwarz, N. (1994). Judgment in a social context: Biases, shortcomings, and the logic of conversation. *Advances in Experimental Social Psychology*, *26*, 123–162.

Schwarz, N. (1995). What respondents learn from questionnaires: The survey interview and the logic of conversation. The 1993 Morris Hansen Lecture. *International Statistical Review*, *63*, 153–177. https://doi.org/10.2307/1403610

Schwarz, N. (1996). *Cognition and communication: Judgmental biases, research methods and the logic of conversation*. Hillsdale, NJ: Erlbaum.

Schwarz, N., & Lee, S. W. S. (2019). The smell of suspicion: How the nose curbs gullibility. In J. P. Forgas, & R. F. Baumeister (Eds.), *The social psychology of gullibility: Fake news, conspiracy theories, and irrational beliefs* (pp. 234–252). New York, NY: Routledge/Psychology Press.

Smith, G., & Oyserman, D. (2015). Just not worth my time? Experienced difficulty and time investment. *Social Cognition*, *33*, 85–103. https://doi.org/10.1521/soco.2015.33.2.1

Sperber, D., & Wilson, D. (1995). *Relevance: Communication and cognition* (2nd edn). Oxford: Blackwell Publishing.

Stinnett, R., Hardy, E., & Waters, R. (2013). Who are we? The impacts of anthropomorphism and the humanization of nonprofits on brand personality. *International Review on Public and Nonprofit Marketing*, *10*, 31–48. https://doi.org/10.1007/s12208-012-0087-z

Thomaz, F., Salge, C., Karahanna, E., & Hulland, J. (2020). Learning from the Dark Web: Leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science*, *48*, 43–63. https://doi.org/10.1007/s11747-019-00704-3

Yan, V., & Oyserman, D. (2020). Linking mindsets to toolsets: difficulty mindsets matter for knowing how to learn. Manuscript under editorial review.