Forthcoming: Journal of Consumer Psychology, 2020

Journal of Consumer Psychology
30.4 (2020): 780-783
https://doi.org/10.1002/jcpy.1187

Reasons for Both Pessimism and Optimism: A Response to the Commentaries (Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age)

Alessandro Acquisti, Laura Brandimarte, and George Loewenstein[1]

Authors' version. Not final

We had thought that our piece presented about as bleak a picture of the current privacy climate as could be imagined. These three superb commentaries, however, suggest that we may have fallen short of plumbing the depths of the current problem. Yet, if they are, possibly, even more despairing than we are about the current state of affairs, we read these commentaries as more optimistic about the prospects for an improvement of the situation. For instance, it is certainly encouraging to see some litigation outcomes going in favor of consumers, as Jagadish points out. Likewise, Mulligan, Regan, and King (MRK) propose that the very bleak current state of privacy is reinvigorating a collective interest in protection against surveillance. Even Oyserman and Schwarz can be seen as optimistic about the prospects for positive progress in the sense that they propose that public information campaigns could yield substantial benefits.

Privacy, as Jagadish highlights, has always been a nuanced concept. As also our review emphasizes, privacy protection cannot be conceived of as an on-off switch. Privacy protection is about the management of information flows within and across what Jagadish refers to as "circles," or Nissenmbaum would refer to as contexts, or Altman and later Petronio would refer to as "boundaries." It is precisely this type of management that is made increasingly difficult for consumers given, on the one hand, technological progress facilitating profitable data harvesting, and, on the other hand, lack of regulation of the data market.

In fact, as pointedly noted by Jagadish, it may be perfectly rational for consumers not to bother reading all privacy policies of providers of goods and services: all those policies are most likely quite similar to

[1] Acknowledgments: We thank Aradhna Krishna and two anonymous reviewers for their sharp and insightful guidance. We thank Ross Anderson, Julie Cohen, Jessica Colnago, Lorrie Cranor, Daphne Chang, Judith Donath, Alisa Frik, Jim Graves, Chris Hoofnagle, Wolfgang Kerber, Steve Margulis, Kirsten Martin, Eyal Peer, Sandra Petronio, Elissa Redmiles, Florian Schaub, Daniel Solove, and Daniel Smullen for their time and their helpful comments. Some arguments in Section 4 are based on remarks prepared by one of the authors for the Atlanta FED 2019 Conference on Markets and the Economy. Acquisti gratefully acknowledges support via a grant from the Alfred P. Sloan Foundation.

each other. That is also the conclusion of our review of the economic theory behind privacy protection. Dominant firms on the market have essentially established norms of data use via self-regulation which are too often directed at maximizing short-term profits from data collection and exploitation instead of developing long-term relationships built on mutual trust, respect of (digital) rights, and loyalty (see a recent piece by Richards and Hartzog 2020). Once such norms are established, there is essentially nothing consumers can do but accept them, since all other competitors will have followed suit, causing a homogeneity of practices on the supply side which also discourages any potential entrant from trying to run their business differently.

Companies' incentives are often not aligned with their customers'. One good example is what Jagadish refers to as the death of a business: "When companies go out of business, their data assets are monetized by their creditors." But a company does not even have to disappear from the market in order for such misalignments to become evident. What typically happens when there is a merger or an acquisition, for instance, is complete sharing of customers' data available to both sides—something that consumers are highly unlikely to consider when they decide to share information with a business.

After reviewing the current state of privacy, including the profound observation that companies use the insights they gain from consumer data not only to understand, but actually to shape, consumer preferences, MRK cite Altman to remind us that privacy is also "'an interpersonal event, involving relationships among people' centered not in individual control but in social negotiation." They argue that, while individual, "atomistic" interests in privacy (such as those our review focused on) may fail to motivate political action, the very hurdles that the modern consumer faces when dealing with privacy, and which our piece extensively catalogued, can foster a collective resurgence of interest in privacy "as a means to address the wealth of harms these conditions produce."

We fundamentally agree with MRK about the importance of the social, collective, dimensions of privacy. At the same time, we see problems in applying Altman's insight on privacy as an interpersonal process to the current privacy climate, without additional caveats. We referred to those problems in our review: "[t]he consumer seeking privacy in the digital age cannot rely on Altman's mutually shared social norms and intuitive behaviors, which worked in an offline world. S/he is a modern Sisyphus constantly forced to learn new strategies, to little avail." In other words, the pre-Internet world in which direct personal interactions constituted the predominant (albeit not necessarily the only) domain of privacy negotiations—a world of mostly person(s)-to-person(s) interactions, where instincts and norms guided both privacy-seeking and privacy-conferring behaviors[2]—is a very different world, privacy-wise, from the one we live in now. In our world, person-firm interactions are ubiquitous and marked by exceptional degrees of information asymmetry, imbalance of power, lack of shared social norms between the individual and the corporation, and thus, ultimately, lack of reciprocity. In fact, in our world, even person-to-person interactions have become organization-mediated: More and more one can say that human-to-human communication is, in fact, computer-mediated (and therefore service providers-mediated) interaction. We agree with MRK that the current state of privacy has "left no space for privacy as a lived, intuitive, human practice." Yet, while MRK draw the optimistic conclusion that the ensuring vacuum can foster a resurgence of interest in privacy, we fear that this resurgence itself may be muted, or diverted, by the very forces (behavioral and economic) we catalogued in our review—

[2] An Altmanian example would be lowering or diverting one's gaze to avoid directly staring or glaring at a stranger.

because those forces (and the service providers behind them) have interposed themselves deeply into the way privacy is socially negotiated between individuals. Consider, again, the many ways social media interfaces direct and, to some extent, dictate both the modes and contents of interactions between individuals, and in turn how those platform-mediated interactions may end up influencing events well beyond the confines of those digital platforms (as in the Cambridge Analytica example that opened our piece).

MRK cleverly build on our reference to privacy economic "dark matter" (the vital dimensions of privacy that economics cannot quantify, such as privacy as a human right, privacy as freedom, dignity, and so forth), and argue that collective unhappiness about invasions of these non-economic dimensions of privacy can potentially spur calls for enhancements in privacy protection. Our own perspective is more pessimistic. Our use of the "dark matter" concept was in part intended to convey that these are aspects of privacy that, despite their higher importance, may be less salient in consumer decision making. And our objective in putting forward the dark matter analogy was also grounded in the observation that, parallel to the important advancements on the economics of privacy and personal data in the last two decades (which we see as useful intellectual progress), there has been also an increasing temptation in some policy circles to rely almost exclusively on economic arguments to resolve policy issues surrounding privacy (which we see, instead, as an unalloyed deterioration in the debate surrounding privacy). In other words, the very (and to a large degree, deserved) success of this particular field of research may have had the undesirable and unintended effect of giving credence to the notion that economic metrics are *the* ultimate metrics to apply in judging questions of privacy policy. The position that, unless there are demonstrable, provable, and quantifiable economic costs from privacy invasions then there are no costs worth paying attention to, is—in our view—obviously false and dangerous. In fact, our essay attempts to highlight the nuanced implications of privacy protection for different stakeholders, the fact that those implications are often not economic in nature, and the fact that so-called privacy trade-offs (be them monetary or not) can be improved by proper use of technology and regulation.

Oyserman and Schwarz draw attention to the idea that companies deliberately focus consumers' attention on specific dimensions of privacy, such as those affecting the security of payments, and away from the types of dimensions we have encompassed with the term "dark matter," in part because the former are the elements of privacy that are probably best-protected (because it is in the economic interests of companies to do so) and in part because doing so distracts consumers from dimensions of privacy that, though arguably just as, or even more, important, firms are wary of protecting.

Oyserman and Schwarz identify an important range of tactics used by firms to encourage disclosure, focusing especially on those employing the increasingly human-like nature of the web interfaces we interact with, and, as a result, the unconscious assumption that communications are following conversational norms that derive from our associations with other individuals. We agree that this is an important psychological factor that is driving developments in online settings. For example, who could have anticipated that products such as Alexa and Siri, that are constantly listening in on one's daily conversations, would be admitted so readily to massive numbers of households. The concepts of anthropomorphism and conversational norms help to explain why this occurred, and also suggests that future developments along these lines, which will certainly become even-more human-like, are likely to meet with similar or even greater levels of acceptance. Oyserman and Schwarz make a number of

interesting and original points, many of them supported by their own research that their commentary provides a detailed review of. For example, while apps and the platforms they run on (e.g., smartphones) are probably best viewed as tools for accomplishing diverse tasks, people instead tend to naturally view them more like friends, or even extensions of the self, and hence as reflections of their personal identity. Apps are also designed to distract attention from some dimensions of privacy (e.g., the sharing of location data) by focusing on others (e.g., protection of payment information). If there is an aspect of their commentary that we disagree with (as we have already hinted at), it is their conclusion. In a section titled "Next Steps," Oyserman and Schwarz focus on the need for public information campaigns to inform consumers about what online transactions entail. Although we are not opposed to such campaigns, our commentary explains why we are very skeptical that these types of informational interventions can make much if any of a dent on the problem of loss of privacy.

In closing, we want to draw attention to a few points that the three superb commentaries led us to ponder.

First, we, and to varying extents the commentators, present a stark contrast between firms, which are seen as deliberate, crafty and manipulative, and consumers, who are presented as conflicted, possessing an inborn desire for privacy yet shedding personal data in a seemingly unconcerned fashion. This dichotomous perspective probably imbues firms with greater rationality and craftiness than they merit. Firms, like consumers, are almost certainly "winging it" to a great extent—trying out different approaches, sticking with those that benefit the bottom line, and dropping those that don't. The end result of this evolutionary process, however, is one that increasingly benefits the fitness of firms at the expense of consumers.

Second, our hope is that research in this area may ultimately change the frame of the public debate surrounding privacy: Rather than unquestionably accepting the premise that loss of privacy is necessary to enjoy the benefits of data, or at the opposite extreme calling for radical privacy protections whatever their cost, we should ask: are there approaches to the regulation of privacy that could enable society to realize the greatest benefits from data sharing while simultaneously protecting privacy in the ways that matter most? New technologies, as well as promising results from economic analysis, suggest that this may be possible.

Third, much as dark matter may encompass a majority of the matter in the universe, so privacy dark matter may account for the most important aspects of privacy that have been lost and that society would benefit from reclaiming. As we noted above, the success of the economics of privacy as a field of research does not justify the conclusion that economic metrics are the only, or ultimate, metrics to apply in judging questions of privacy policy. To paraphrase Georges Clemenceau: privacy is too serious a matter to entrust to us economists alone.

Are there, then, any grounds for hope in this seemingly bleak privacy landscape?

We are perhaps a bit more agnostic than MRK regarding the chances that collective efforts, including "external and internal constituencies" that "push back on surveillance practices," will overcome enormous corporate interests and incentives. We *wish* this were the case, but we also wonder, and fear, whether seemingly favorable recent developments (such as those involving IBM and Microsoft, mentioned by MRK) are temporary, fleeting exercises in PR, fragile barriers that may fall again under the pressure of the unavoidably adaptive nature of privacy norms and behaviors. And yet, we do share some

of that optimism with MRK—as we do with similarly hopeful notes in Jagadish and in Oyserman and Schwarz. As we noted in our conclusive section, we too believe that progress is possible, if for no other reason than the fact that privacy appears to be a fundamental need and drive of human nature. And that is where research in several fields could play a productive role. There is so much we do not know yet about the economic, social, behavioral, technological impacts of privacy regulation. Further understanding and deeper knowledge of the impact of privacy protection is what we ultimately advocate for.

References

Richards and Hartzog, "A duty of loyalty for privacy," July 3, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217.