aps ASSOCIATION FOR PSYCHOLOGICAL SCIENCE

Current Directions in Psychological Science
2021, Vol. 30(2) 159–166


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0963721421990355
www.psychologicalscience.org/CDPS
SAGE

The Privacy Mismatch: Evolved Intuitions in a Digital World

Azim Shariff[1], Joe Green[2], and William Jettinghoff[1]
[1]Department of Psychology, University of British Columbia, and [2]School of Psychology, University of Sussex

Abstract
Although people report grave concern over their data privacy, they take little care to protect it. We suggest that this *privacy paradox* can be understood in part as the consequence of an evolutionary mismatch: Privacy intuitions evolved in an environment that was radically different from the one found online. This evolved privacy psychology leaves people disconnected from the consequence of online privacy threats.

Keywords
emotion, evolution, Internet, privacy, technology

"You have zero privacy anyway," declared Scott McNealy, CEO of Sun Microsystems in 1999. "Get over it" (quoted in Sprenger, 1999, paras. 1–2). Two decades later, the amount of public data vacuumed up by social networks, geolocalized cell phones, and other smart devices makes those early days seem quaint. Yet polling indicates that people remain strongly—indeed, increasingly—concerned about online privacy (Pew Research Center, 2019). They have not "gotten over it." Or at least, they say they have not. Though people express serious concerns about their privacy, these same people do little to protect it (Gerber et al., 2018). This inconsistency—now extensively documented (Kokolakis, 2017)—is known as the *privacy paradox*.

As more of people's lives moves online and falls under increasingly sophisticated surveillance technologies, these gaps between the public's professed desire for privacy and their behavior will become more consequential. We argue here that understanding privacy psychology in modern online environments requires looking back to the evolutionary roots of privacy concern. The privacy paradox, we submit, is the consequence of an evolutionary mismatch (Li et al., 2018). Human privacy intuitions emerged in an ancestral environment that differed radically from the digital environment in which those intuitions are now being tested.

The Privacy Paradox

Privacy is broadly defined as having control over others' access to the self (Altman, 1975), but it is often divided into different dimensions (Table 1). The privacy paradox focuses specifically on the gap between expressed and revealed preferences when it comes to *informational* privacy. In one study, Facebook users were asked how concerned they would be if strangers could freely access information indicating their sexual and political orientation. Of those participants reporting the very highest level of concern, 48% nonetheless self-disclosed their sexual orientation, and 47% self-disclosed their political orientation (Acquisti & Gross, 2006). The paradox holds even for people with strong technological knowledge and high awareness of privacy risks (Barth et al., 2019) and has been shown across e-commerce, financial services, social-networking sites, and mobile-app downloads.

There are several ways to understand the paradox. Among the most notable has been the *privacy-calculus theory* (Dinev & Hart, 2006): Humans, as rational actors, weigh the expected costs of a loss of privacy against the benefits that the disclosure provides. In this view, there is no paradox; rewards derived from self-disclosure may be difficult to articulate but are worthwhile enough to people to justify the privacy costs. Other researchers, more skeptical about the "homo economicus" view of people as entirely rational agents, instead highlight the role of cognitive biases; people's tendency to discount the future (Hallam & Zanella, 2017), to be overly optimistic

Corresponding Author:
Azim Shariff, Department of Psychology, University of British Columbia
E-mail: shariff@psych.ubc.ca

Table 1. Four Dimensions of Privacy, Based on Burgoon (1982)

Dimension	Description
Physical privacy	The use of spatial distancing and physical barriers to regulate exposure from surveillance as well as physical proximity to other people
Social privacy	The interactional aspects of privacy, including intimate social engagement with select individuals plus some form of separation from others
Psychological privacy	The ability of individuals to avoid unwanted interruption and be free to contemplate, concentrate, introspect, etc.
Informational privacy	The ability to regulate the collection and dissemination of information about oneself

about their own outcomes compared with others' (Cho et al., 2010), and to underestimate the risks of things that elicit positive emotions (Kehr et al., 2015) all result in privacy behavior that is laxer than stated privacy preferences.

The privacy paradox likely has many causes. However, we suggest that a more complete account of the paradox benefits from taking a functionalist approach to why people care about privacy to begin with. We argue that millions of years of complex interpersonal interaction have left humans with a suite of privacy-based intuitions that help regulate both physical and psychological boundaries. These evolved intuitions are heuristically elicited by a variety of social stimuli and backed by aversive emotional reactions. Yet the effectiveness of these psychological adaptations is curtailed in the novel and rapidly evolving digital environment. Although in the abstract people may rationally recognize threats to their privacy online, the online world fails to elicit the emotional reaction—and thus the motivational force—to reliably compel behavior change. To understand when privacy violations do and do not evoke strong reactions, it is useful to examine the underlying functions these reactions evolved to serve.

The Evolution of Privacy

Evolutionary theorizing about privacy often draws direct analogies (when evolved phenomena serve common functions) and/or homologies (when evolved phenomena have common origins) between human privacy concern and proto-privacy concerns seen across the nonhuman animal kingdom (Klopfer & Rubenstein, 1977). For both human and nonhuman species, controlling the boundaries between self and others serves critical fitness goals. Personal space (the interpersonal distance at which an organism feels comfortable) and territoriality (a defendable bounded geographic area) are two common forms of these boundaries. Each involves a safety buffer from threats to the self and vital resources, and both are seen recurrently across the animal kingdom (Westin, 1967). Because social interaction is often also crucial to fitness, organisms have faced evolutionary pressures to develop psychological mechanisms to flexibly regulate social boundaries—carefully balancing approach and withdrawal, interaction and seclusion.

As theory of mind, language, and social complexity increased among humans and their recent ancestors, fitness came to additionally depend on the maintenance of cooperative social relationships—and thus the maintenance of an individual's social reputation (Van Vugt et al., 2007). As a result, in addition to regulating access to self and territory, individuals are likely to have benefited from controlling and manipulating access to reputation-relevant information. Given the incentive to manage this information, privacy concern may have evolved to motivate the individual to avoid the threat of unregulated or unwanted access to information about the self.

Reports of impression-management tactics being used by humans' closest nonhuman relatives support this idea. To establish dominance without fighting, chimpanzees often engage in face-to-face mutual bluff displays. However, chimps involuntarily bare their teeth when frightened, a reflex that undermines a dominant appearance. De Waal (1986) observed chimps turning their backs until this reaction subsided, shielding it from their competitors' view. This is a rudimentary form of informational privacy. However, such tactics are orders of magnitude more elaborate among humans, who not only reliably modify their behavior when they know they are being observed, but also carefully cultivate their reputations by strategically manipulating (deception), displaying (signaling), and withholding (privacy) information about themselves.

Integrating these theoretical lines, we propose that for humans, privacy concerns evolved to protect bodily, territorial, and reputational integrity from recurrent ancestral challenges. We suggest that psychological mechanisms of privacy concern evolved in small-group environments to reflexively respond to two main challenges: avoiding nearby potential threats and avoiding reputational damage. Adaptive behaviors—such as increasing interpersonal distance or decreasing self-disclosure and exposure—evolved to protect the self

and were reliably triggered by a specific set of social and environmental cues.

Norms about what was socially acceptable, and eventually, laws about what was legally permissible, emerged to regulate wider social arrangements that balanced the preferences of the individual with the interests of the group. Though this balance had privacy intuitions as its psychological foundation, the diverse local ecologies and histories faced by different societies led to notable cultural variability in privacy norms, even while core privacy concerns remained universal (Altman, 1977). Today's online environment, however, has strayed far from both the ancestral environment to which privacy intuitions adapted and the cultural environment from which privacy norms emerged.

Evolutionary Mismatch

An evolutionary mismatch occurs when an environmental change leaves a once-beneficial trait unable to fulfill the function that led it to be selected (Cofnas, 2016). The fearlessness of birds that evolved on remote islands, far from mammalian predators, becomes maladaptive when mammals are introduced (Lloyd et al. 2014). A taste for fat and sugar, calibrated for an environment in which these are scarce, becomes maladaptive when civilization makes them abundant (Li et al., 2018). These examples show the misalignments that occur when a psychology calibrated for one environment then faces another. The arrival of social media, mass facial recognition, and ubiquitous smartphones with tracking and eavesdropping capability has created a similarly novel environment. This abrupt switch from face-to-face to digital has stripped the social environment of many of the cues required to trigger people's intuitions regarding privacy violation (e.g., the visceral reaction to noticing a stranger reading your texts over your shoulder is likely absent when the same information is even more visibly shared online). People's carefully calibrated privacy psychology is left ill equipped to deal with 21st-century security challenges. In this section, we specify three specific psychological mismatches: ownership psychology, personal space, and reputational concerns (Fig. 1).

Ownership psychology

Beyond simply possessing things, humans also own things; they develop and respect rules of ownership to improve social coordination (Nancekivell et al., 2019). Indeed, it has been argued that the concept of ownership evolved in response to the challenge of avoiding recurrent and costly disputes over resources such as territory and food (Boyer, 2015). And although extensive meat sharing was common among early hunter-gatherer communities, and ownership was rare, this scenario was sustained only under strict culturally enforced sharing norms to support large groups and suppress personal stockpiling. As humans began to live in more permanent settlements, such norms were relaxed, which allowed the latent ownership psychology to reemerge.

Today, the concept of ownership is present in nearly all existing human languages and cultures, and it has been shown to emerge early in childhood (Boyer, 2015). Two-year-olds already infer ownership of objects, and 4-year-olds can discern ownership on the basis of investment of labor, refraining from taking resources accordingly (Kanngiesser et al., 2020). In adolescence, the things an individual owns can be enveloped into his or her identity—creating an "extended self" (Belk, 2018). We suggest that privacy intuitions evolved to selectively control access not just to the physical self, but also to this extended self, including territory, possessions, and even intellectual property.

However, establishing who owns what can be challenging. To do so, people intuitively rely on a complex set of ownership cues. Cues including who first possessed an object or who contributed the labor to make or modify something help people intuit ownership (Nancekivell et al., 2019). But unlike interpersonal environments, digital environments often lack these cues. For example, in the case of a GPS app, who is the first possessor of users' location data—the users or the app? Whom do the users attribute labor investment to—themselves or the software developers? Such online ambiguity produces an evolutionary mismatch: Opaque ownership cues in the digital environment often fail to prompt the privacy intuitions necessary to motivate personal data-protection behavior.

Personal space

Through largely unconscious cognitive processing, both humans and nonhuman animals are continually navigating their social space so as to maintain a safe and comfortable distance between themselves and others. This space—personal space—provides not just a defense mechanism against incoming attack or collision, but also a level of physical privacy to help regulate stress and emotion (Vagnoni et al., 2018). The size of this safety zone is determined by intrapersonal, interpersonal, and environmental variables. Interpersonal determinants such as aggressive conversations (Vagnoni et al., 2018), emotional faces (Ruggiero et al., 2017), and others' age (Iachini et al., 2016) can all modulate the size of personal space. Yet most nonverbal cues disappear when three-dimensional social environments collapse into two-dimensional online environments.

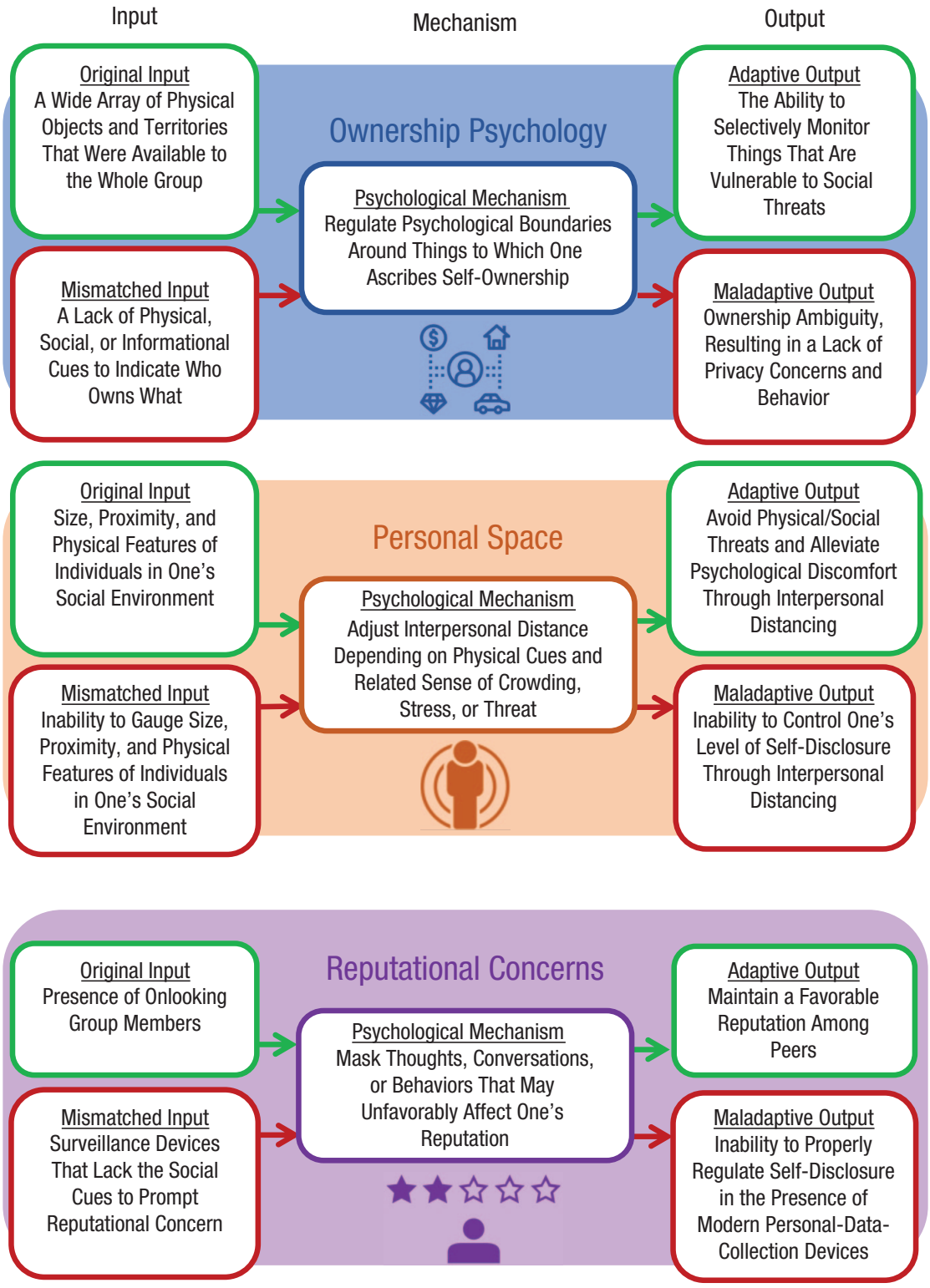

Fig. 1. Evolutionary mismatch in ownership psychology, personal space, and reputational concerns. For each mechanism, the figure shows the input and output of a process that was adaptive in humans' ancestral environment (green) and the input and output of a process that is maladaptive, because of evolutionary mismatch, in the novel modern environment (red).

The emergence of platforms like Twitter and Facebook suddenly enabled people to connect and share with millions of other people worldwide. This stands in stark contrast to the relatively small in-person social networks of humans' ancestral (or even recent) past. In this new form of technology-mediated communication, users often self-disclose to a large, unseen, and heterogeneous group (Lieberman & Schroeder, 2020). By replacing an observable audience with an imagined one, individuals lose a complex set of social response cues that they would typically and reflexively use to guide their self-disclosing behavior toward people perceived as receptive or friendly and away from those perceived as unreceptive or hostile. Consequently, a regrettable late-night tweet becomes more likely when one is faced with a static screen instead of a thousand expressive onlookers. Without face-to-face interaction, social-media interfaces do not allow people to emotionally register reliable signals of potential social threat, such as crowding or overstimulation. In turn, people fail to reduce their interpersonal exposure—perhaps the most basic form of privacy protection.

Reputational concerns

As was true for paleolithic hunter-gatherers, modern-day Internet users face the consequences of the impressions that other people form and share about them. Research from various disciplines has shown how individuals condition their cooperation or punishment toward another person according to that person's reputation from previous interactions, observations, and third-party gossip. Humans have thus evolved a complex reputation-management psychology.

We suggest that privacy concerns are one component of this psychology, motivating individuals to control and conceal socially damaging information or behavior. And although social-media sites may lack many useful social cues, alerts and notifications do at least remind users of the presence of observers. These gentle reminders are often enough to motivate users to apply some privacy measures, albeit imperfectly, to protect their online reputation. However, an emergent field of technology is now collating enormous amounts of users' data, effectively invisibly.

The *Internet of things* (IoT) refers to a system of interconnected devices, from smart refrigerators to fitness trackers, that collect and share data via the Internet. By 2018, approximately 18 billion IoT devices worldwide were already in use, amassing users' personal data (Statista, 2020). Many reports of privacy risks and violations—such as eavesdropping by smart speakers in people's homes—have emerged. Despite this, studies have found that although privacy concerns reduce social-media use (Jozani et al., 2020), they do not affect intentions to purchase IoT devices (Menard & Bott, 2020). From the evolutionary perspective, differences in reputational cues between IoT devices and social media can account for differences in users' privacy concerns and behaviors.

Unlike on social media, reputational cues are almost entirely absent with IoT devices; once configured, these largely silent, faceless, smart devices continuously and imperceptibly collect personal data outside of conscious awareness. In addition, this information is then fed to a faceless corporation's database, rather than to identifiable individuals in one's extended social circle. Therefore, though the IoT may prompt nominal and abstract privacy concerns, because it does not stir real reputational concerns, users' visceral privacy intuitions remain sidelined.

A Future

For privacy psychology, the past three decades have seen an environmental change that is arguably larger than even the Neolithic revolution 12,000 years ago. In this current environment, online interfaces befuddle intuitions that have otherwise allowed people to adaptively decide what to share, how much, and with whom. The mass, permanent record of online behavior leaves access to people's information—and thus control over their reputations and decisions—to the whims of online power brokers. This leaves users vulnerable to coercive persecution by dissent-averse governments, commercial manipulation by profit-seeking corporations, and criminal exploitation by tech-savvy ne'er-do-wells (Zuboff, 2019).

Examples of the consequences of privacy erosion are accumulating. Data breaches have taken a substantial psychological and human toll (the leaking of account information from adulterous match-making site Ashley Madison provoked divorces, resignations, and suicides). The easily accessed digital footprints people leave online can often return to sabotage other aspects of their life (e.g., Sherman, 2013, found that one in ten 16- to 34-year-olds reported being rejected from a job because of something they had posted online). Surreptitiously acquired personal data on Facebook can be used to sway an electorate (as happened in the 2016 U.S. election with the political consulting firm Cambridge Analytica and the Trump campaign). Perhaps the most large-scale example is the broad use of online data that powers China's Social Credit System, which has already been used to regulate millions of citizens' travel options, apartment rents, medical wait times, and even education quality.

However, people's reactions to privacy violations are tied not to these grave consequences, but to their

evolved intuitions. This disconnect between reaction and consequence exposes how privacy psychology can be exploited for power and profit. For instance, even though technology companies soberly and technically explain their privacy policies, they can nonetheless easily coax data from people by burying the cues that would trigger evolved privacy concerns. In exchange, companies offer returns—for example, the connection of social networks or the titillation of online pornography—that powerfully appeal to evolved desires. Both corporations and governments often appease citizens' civil-liberty concerns by removing the triggers of, rather than the actual intrusions behind, privacy concern. These types of solutions exploit humans' mismatched psychology, quelling immediate emotional reactions while leaving the deeper, more rational concerns unaddressed.

Evolutionary mismatches tend to resolve via subsequent evolution, environmental change, or behavioral adaptation (Lloyd et al., 2014. The glacial pace of genetic evolution precludes subsequent evolution from being a reasonable solution for this issue. Environmental change, in this context, would entail changing how people experience the Internet. Europe's General Data Protection Regulation was aimed at such user-level changes, but its contractual legalese bloodlessly appealed only to abstract concerns, failing to ignite emotional privacy intuitions. Privacy alerts could be reimagined to more viscerally trigger people's social intuitions (Calo, 2012), and researchers should measure the effectiveness of such changes for aligning preferences and behavior. However, we are pessimistic.

The sheer scale of privacy management online makes putting the behavioral onus on individual users—even with the help of alerts and pop-ups on websites—unrealistic. The problems are similar, if even more formidable, for bottom-up behavioral adaptations that require individual users to simply edit their privacy settings themselves. Even scholars who are themselves skeptical of the existence of a privacy paradox (e.g., Solove, 2020) recognize that when it comes to privacy, the online environment is too vast to be individually managed given humans' psychological limitations. People were not built for it.

Given the privacy mismatch, efforts to align users' preferences and behavior may prove futile. A more tractable solution could focus on mitigating the negative consequences of people's loose privacy behavior, but data-protection efforts face resistance from powerful government and corporate interests. Challenging those interests would require rousing public interest in, and changing social norms about, data privacy. Psychologically, one strategy for lifting an issue to sociopolitical importance is via "moral piggybacking"—tying privacy to other areas of existing moral concern (Feinberg et al., 2019). Privacy could be piggybacked on fairness concerns, by highlighting the injustice of corporations extracting personal data for profit, or onto liberty concerns, by reminding people that their data fuel mass manipulation through personalization algorithms. Moralizing privacy via piggybacking may rally greater political will to support privacy rights.

Obviously, the online environment is vast and diverse. Not all domains will lead to poorly calibrated oversharing. In fact, certain technologies may provoke mismatches that err in the other direction, affording novel but self-defeating motivations for social withdrawal. For instance, videoconferencing enables asymmetric visibility whereby students, patients, or audience members can unilaterally disable their webcams—rendering themselves seeing, but unseen. This protects privacy, but may undermine other goals by degrading a traditional social experience.

In either case, for something so morally complex, culturally ubiquitous, and increasingly topical, privacy somehow remains understudied in psychology. We hope that the functionalist approach we have outlined here can help close the gap between the paucity of psychological research on privacy and the important, pervasive, and ever-widening public discussion of it. There are few topics for which the gap is so large.

Recommended Reading

Klopfer, P. H., & Rubenstein, D. I. (1977). (See References). One of the few evolutionary accounts on the origins of privacy concern in humans and nonhuman animals.

Kokolakis, S. (2017). (See References). A comprehensive (up to its publication date) review of the privacy paradox, including an overview of the empirical research and attempts at explanations.

Li, N. P., van Vugt, M., & Colarelli, S. M. (2018). (See References). A brief but very useful review of the concept of evolutionary mismatches, including many examples relevant to psychology.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, *126*(7), 1934–1965. A seminal article explaining the consequences of deteriorating privacy in the face of emerging technologies.

Solove, D. J. (2020). (See References). An article that provides a more skeptical view of the privacy paradox, as well as a smart outline of the challenges in leaving online privacy management to individual users.

Transparency

Action Editor: Robert L. Goldstone
Editor: Robert L. Goldstone
Declaration of Conflicting Interests
The author(s) declared that there were no conflicts of interest with respect to the authorship or the publication of this article.

ORCID iD

Azim Shariff https://orcid.org/0000-0003-4444-460X

Acknowledgments

A. Shariff and J. Green contributed equally to this work.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy enhancing technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, revised selected papers* (pp. 36–58). Springer.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory and crowding*. Brookes.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66–84.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69.

Belk, R. (2018). Ownership: The extended self and the extended object. In J. Peck & S. B. Shu (Eds.), *Psychological ownership and consumer behavior* (pp. 53–67). Springer.

Boyer, P. (2015). How natural selection shapes conceptual structure: Human intuitions and concepts of ownership. In E. Margolis & S. Laurence (Eds.), *The conceptual mind: New directions in the study of concepts* (pp. 185–200). MIT Press.

Burgoon, J. K. (1982). Privacy and communication. *Annals of the International Communication Association*, *6*(1), 206–249.

Calo, M. R. (2012). Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, *87*(3), 1027–1072.

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995.

Cofnas, N. (2016). A teleofunctional account of evolutionary mismatch. *Biology & Philosophy*, *31*(4), 507–525.

De Waal, F. (1986). Deception in the natural communication of chimpanzees. In R. W. Mitchell & N. S. Thompson (Eds.), *Deception: Perspectives on human and nonhuman deceit* (pp. 221–244). State University of New York Press.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Feinberg, M., Kovacheff, C., Teper, R., & Inbar, Y. (2019). Understanding the process of moralization: How eating meat becomes a moral issue. *Journal of Personality and Social Psychology*, *117*(1), 50–73.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227.

Iachini, T., Coello, Y., Frassinetti, F., Senese, V. P., Galante, F., & Ruggiero, G. (2016). Peripersonal and interpersonal space in virtual and real environments: Effects of gender and age. *Journal of Environmental Psychology*, *45*, 154–164.

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, *107*, Article 106260. https://doi.org/10.1016/j.chb.2020.106260

Kanngiesser, P., Rossano, F., Frickel, R., Tomm, A., & Tomasello, M. (2020). Children, but not great apes, respect ownership. *Developmental Science*, *23*(1), Article e12842. https://doi.org/10.1111/desc.12842

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635.

Klopfer, P. H., & Rubenstein, D. I. (1977). The concept privacy and its biological basis. *Journal of Social Issues*, *33*(3), 52–65.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134.

Li, N. P., van Vugt, M., & Colarelli, S. M. (2018). The evolutionary mismatch hypothesis: Implications for psychological science. *Current Directions in Psychological Science*, *27*(1), 38–44. https://doi.org/10.1177/0963721417731378

Lieberman, A., & Schroeder, J. (2020). Two social lives: How differences between online and offline interaction influence social outcomes. *Current Opinion in Psychology*, *31*, 16–21.

Lloyd, E., Wilson, D. S., & Sober, E. (2014). *Evolutionary mismatch and what to do about it: A basic tutorial*. Evolution Institute. https://evolution-institute.org/wp-content/uploads/2015/08/Mismatch-Sept-24-2011.pdf

Menard, P., & Bott, G. J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security*, *95*, Article 101856. https://doi.org/10.1016/j.cose.2020.101856

Nancekivell, S. E., Friedman, O., & Gelman, S. A. (2019). Ownership matters: People possess a naïve theory of ownership. *Trends in Cognitive Sciences*, *23*(2), 102–113.

Pew Research Center. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Ruggiero, G., Frassinetti, F., Coello, Y., Rapuano, M., Di Cola, A. S., & Iachini, T. (2017). The effect of facial expressions on peripersonal and interpersonal spaces. *Psychological Research*, *81*(6), 1232–1240.

Sherman, E. (2013, June 4). *1 in 10 young job hunters rejected because of their social media*. AOL. https://

www.aol.com/2013/06/04/applicants-rejected-social-media-on-device-research/

Solove, D. J. (2020). The myth of the privacy paradox. *George Washington Law Review*, *89*. https://doi.org/10.2139/ssrn.3536265

Sprenger, P. (1999, January 26). Sun on privacy: 'Get over it.' *Wired*.

Statista. (2020). *Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030*. https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

Vagnoni, E., Lewis, J., Tajadura-Jiménez, A., & Cardini, F. (2018). Listening to a conversation with aggressive content expands the interpersonal space. *PLOS ONE*, *13*(3), Article e0192753. https://doi.org/10.1371/journal.pone.0192753

Van Vugt, M., Roberts, G., & Hardy, C. (2007). Competitive altruism: Development of reputation-based cooperation in groups. In D. M. Buss (Ed.), *Handbook of evolutionary psychology* (pp. 531–540). John Wiley & Sons.

Westin, A. (1967). *Privacy and freedom*. Athenaeum.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Hatchett.