Available online at www.sciencedirect.com

ScienceDirect

Current Opinion in Psychology

Privacy matters . . . or does It? Algorithms, rationalization, and the erosion of concern for privacy

Nathanael J Fast and Arthur S Jago

Products and services built around artificially intelligent algorithms offer a host of benefits to users but they require vast amounts of personal data in return. As a result, privacy is perhaps more vulnerable today than ever before. We posit that this vulnerability is not only technical, but psychological. Whereas people have historically cared about and fought for the right to privacy, the diffusion and conveniences of algorithms could be systematically eroding people's capacity and psychological motivation to take meaningful action. Specifically, we examine four factors that increase the tendency to rationalize privacy-reducing algorithms: 1) awareness of the benefits and conveniences of algorithms, 2) a low perceived probability of experiencing harm, 3) exposure to negative consequences only after usage has already begun, and 4) certainty that losing privacy is inevitable. We suggest that future research should consider these and related factors in order to better understand the changing psychology of privacy.

Address
University of Southern California, United States

Corresponding author: Fast, Nathanael J (nathanaf@usc.edu)

Current Opinion in Psychology 2020, **31**:44–48

This review comes from a themed issue on **Privacy & disclosure, online & in social Interactions**

Edited by **Leslie John**, **Diana Tamir**, and **Michael Slepian**

https://doi.org/10.1016/j.copsyc.2019.07.011

> "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life . . . and numerous mechanical devices threaten to make good the prediction that what is 'whispered in the closet shall be proclaimed from the house-tops.'"
> –Samuel Warren and Louis Brandeis, Harvard Law Review (1890)

> "A couple of generations hence, will some automated society look upon privacy with the same air of amused nostalgia we now reserve for, say eighteenth-century drawing room manners?"
> –Myron Brenton, private detective (1964)

Introduction

Understanding and predicting people's attitudes about privacy, both in the present and the future, are important not only to psychologists, but also to businesses, the legal community, and policy makers [1]. Throughout most of modern history, people have fought to protect the right for privacy. For example, Warren and Brandeis's (1890) powerful argument for the 'right to be let alone' has been hailed as one of the most influential law pieces ever written. Half a century later, advocates built upon this foundation, voicing growing concerns about threats to privacy. Their objections were based on the belief that freedom from surveillance is a necessary condition for health and well-being (e.g. [2]), and that a lack of ability to withdraw into privacy might even lead to open hostility [37]. In the present article, we posit that the diffusion and conveniences of automated algorithms are systematically undermining not only people's abilities but also their motivation to protect privacy. We explore the psychology surrounding this phenomenon and call for research aimed at better understanding the relationship between the use of algorithms and concern for privacy.

Algorithms and threats to privacy

In the age of expanding artificial intelligence and machine learning, personal data have become a highly valued commodity. Indeed, in recent years, business leaders and entrepreneurs have repeatedly proclaimed that 'data is the new oil' [3], suggesting that business organizations can become wealthy by creating and maintaining pipelines of personal data that they can then process and sell to advertisers or other interested stakeholders [4,5]. Algorithms, or computerized processes designed to accomplish goals or maximize predictive outcomes [6,7•,8,9•], have become especially useful to companies because they allow organizations to more efficiently collect and process personal information [10,11]. These data are valuable because they can be used to create targeted predictive models about behavior [12,13,14••]. Importantly, algorithms are also useful to companies because they can be used to create benefits that incentivize consumers to willingly share their personal data.

Along with benefits, however, come potential costs. Data, for example, might be used to influence people's attitudes and actions in ways that contradict their values or preferences, and improper data storage and/or sharing can lead to leaks where people's information becomes public and is subsequently stolen, obviously without their

consent. Given the benefits and costs associated with algorithms, people can either choose to accept or fight against their increasing use in both business and society. Here, we propose that the psychological process of rationalization will be a key factor that affects people's willingness to resist such technologies and the privacy violations that accompany them.

Rationalization as a barrier to the motivation to protect privacy

A number of social and psychological forces could lead people to rationalize lower levels of privacy as algorithms proliferate, thereby reducing their chances of engaging in privacy-protecting behaviors. In particular, we posit four likely factors: 1) awareness of the benefits and conveniences of algorithms, 2) low perceived probability of experiencing harm, 3) exposure to negative outcomes only after has usage begun, and 4) certainty that privacy is a foregone conclusion. We posit that each of the following areas represents fertile ground for future research aimed at predicting and understanding people's privacy-related behaviors.

Awareness of the benefits and conveniences of algorithms

Gathering personal data has always benefited organizations but it has not always been evident to people how they, themselves, might benefit from such surveillance. As a result, when people became aware of organizations collecting their personal data, they fought against it (e.g. [15]). With algorithm-based products, however, the benefits and conveniences people earn for providing their data are often both salient and desirable. Algorithms help consumers save time (e.g. on demand transportation, shopping), identify self-relevant content (e.g. music, videos, movies), increase productivity (e.g. digital assistants, behavior tracking), improve decision making (e.g. advice-giving recommendation systems), and connect with audiences (e.g. social media apps). These and other benefits make many algorithm-based products extremely attractive and convenient, creating fertile ground for rationalization (for a review on consumers' attitudes about online privacy, see Ref. [16]), For example, having justifications for problematic behavior makes people more likely to engage in it and minimize evidence regarding its negativity [17–19]. Thus, the conveniences and services algorithms provide might lead people to judge incurred costs—including the potential for privacy violations—in a less negative light, given the benefits bundled alongside them.

One possible issue that could undermine the tendency to rationalize algorithms is the lack (or loss) of awareness of the benefits provided by algorithms. However, given that companies have an incentive to create, maintain, and market the benefits associated with their products, we do not foresee this as a likely possibility.

Low perceived probability of experiencing harm

Further encouraging the rationalization of algorithm reliance is the fact that it is easy to underestimate the likelihood of harm. For example, people tend to see the costs of sharing data as relatively intangible [16,20] and, moreover, companies often intentionally withhold, or make it difficult to obtain, information about exactly how they collect and use data [21]. This lack of concrete understanding of how organizations collect and use personal data may cause people to perceive that harm is relatively unlikely to occur (e.g. Tversky and Kahneman [38]). Consistent with this idea, people often feel freer to share personal information with algorithms and machines (versus with humans) in socially risky situations due to reduced concerns about social evaluation [22–24]. Moreover, when companies anthropomorphize algorithms and machines, this further reduces perceptions of harm by increasing a sense of trust that their interests will be protected [25,26]. As such, people's relatively abstract knowledge of what personal data organizations might have concerning them, how they are using it, and general attitudes towards machine agents all coalesce in ways that might lead people to assume the costs of giving up privacy are both small and relatively unlikely to manifest.

This raises the question of what will happen when harms do, in fact manifest, leading to negative consequences for oneself or others [20]. For example, large data breaches—such as the Equifax breach—could make privacy harms seem more likely or egregious. Another factor that might arrest people's tendency to rationalize costs of privacy reduction is the exposure to *unexpected* risks. Although people might be relatively comfortable sharing their location or search data, they might be less comfortable with algorithms collecting and using data that feels more sensitive, for example, sexual orientation [14••]. However, we suggest that manifestations of harms may not be strong enough to overcome the tendency to rationalize the use of algorithms. This is partly due to a focus on the benefits mentioned earlier and partly due to the fact that realized privacy harms, such as data breaches or leaks, might not always produce explicitly identifiable victims: for example, having only your personal information uploaded to the internet likely produces a different psychological experience than your information being uploaded alongside thousands of other data points [20]. Finally, experiencing harm may not be enough to change behavior, in part, because people have already adopted the algorithms, making it more difficult to give them up. It is to this idea that we turn next.

Exposure to negative outcomes only after usage has begun

While people might underestimate the probability of experiencing harm when using algorithms, it is reasonable to assume that actual realized harms—for example, personal information being uploaded to the internet for

anyone to see following a leak—could produce resistance and catalyze concerns. However, a third factor promoting the rationalization of privacy-reduction is the fact that people's exposure to the negative outcomes associated with sharing their data with algorithms occurs well *after* such a usage has been initiated. People often opt-in to algorithmic systems that collect and use personal data (with some notable exceptions, including the Equifax breach), possibly leading to feelings of commitment to a product or service that persists even when privacy is threatened directly (e.g. [27]).

Recent events offer an imperfect but intriguing test of this idea. In particular, a number of well-publicized events have raised societal awareness of potential and realized dangers of algorithmic privacy violations (e.g. Facebook and the Cambridge Analytica scandal, numerous data breaches, email updates informing users of privacy policy updates after the new GDPR privacy law went into effect in May 2018). By highlighting the potential costs associated with data sharing, such events had the potential to cause backlash and/or reduced willingness to use algorithmic services that involve sharing personal data. However, such backlashes have not been particularly dramatic: Facebook usage purportedly increased following the Cambridge Analytica scandal, and its stock price bounced back relatively quickly following an initial decline [28,29]. These initial responses suggest that consumers might not be prepared to take drastic action to protect their privacy, even when costs become salient (see Ref. [1]). As such, the notion that people are already relying on algorithms might increase psychological pressures to rationalize their continued use, even in the face of realized harm [30].

Certainty that privacy is a forgone conclusion

A fourth factor promoting the rationalization of the use of privacy-reducing algorithms is the perception that such technologies are already a forgone conclusion: a necessity in today's world. Research on rationalization indicates that when a negative outcome has occurred, or is certain to occur, people are more likely to engage in rationalization [31•,32,33]. The rapid proliferation of algorithms in both business and society [34] has not only threatened people's privacy but, somewhat ironically, it may also soon create—or have already possibly created—a situation where people do not believe it is realistically possible to stop data collection efforts and/or usage. Beliefs about the absoluteness of forsaking privacy might only become stronger as new generations grow up in environments increasingly populated by algorithms, leading to even stronger certainty beliefs and possibly subsequent feelings of helplessness [35].

Given research on certainty and rationalization, one possible way to nudge people to protect their privacy is to offer options that allow them to choose higher-privacy algorithmic services instead of lower-privacy ones. In these cases, the perceived certainty of giving up one's privacy might vanish, given that the higher-privacy options ostensibly offer similar services [32,33]. As an example, people prefer gift cards that do not track their purchases over ones that do, even when the more private gift cards are worth less [1]. However, while there are some examples of high-privacy algorithmic options today (e.g. web browsing), organizations are typically not incentivized to offer such options given how useful and profitable collecting and using personal data can. Furthermore, before people act on these choices, they must: 1) be aware of them, 2) experience them as easy and convenient to use, and 3) believe that they provide roughly the same level of benefits as their alternatives (which is often a difficult achievement; how, for example, might a high-privacy social media app compete with Facebook?). Finally, to be meaningful, the privacy protections must be tangible and verifiable as opposed to merely a marketing ploy. For example, any real movement toward higher-privacy options would create incentive for companies to frame their products as high in privacy (or one category of privacy) when in reality (or with regard to other categories of privacy), they are not, leading to illusory perceptions of privacy (see Ref. [36]). Considering these necessary conditions, we are not optimistic that meaningful high-privacy options will emerge for many of the algorithm-based services that people currently use and enjoy.

Conclusion

In this article, we have outlined four factors that might lead to the rationalization of the widespread use and proliferation of algorithms that violate privacy. Although we have proposed that rationalization—and an increased willingness to accept a world without privacy—is likely, it remains an empirical question and it is our hope that the ideas put forth in this article will generate new research in this important area.

As noted, given the strength of the psychological pressures outlined above, we are not optimistic that people will continue to hold privacy as a strong priority. If true, this would point to governmental action as a primary mechanism, by which privacy may be protected. For example, government regulation such as the new GDPR data protection initiatives in the European Union may help protect consumer privacy. However, as mentioned, the endless stream of (primarily unread) emails about updated privacy policies may have only served to increase the rationalization tendencies outlined in our paper, by increasing perceived certainty about the loss of privacy or creating the perception that harms were being eliminated. Thus, it is possible that governmental action must proceed without strong and sustained prodding by the public.

Given the ideas outlined above, people may increasingly rationalize conditions that hinder privacy. Thus, in addition to the above research questions, we would posit that,

to better understand and predict the future of humanity, psychologists may also wish to invest effort into developing and testing theories of human behavior under conditions of little or no privacy.

Conflict of interest statement

Nothing declared.

Acknowledgments

This work is supported by the Air Force Office of Scientific Research, under grant FA9550-18-1-0182. The content does not necessarily reflect the position or the policy of any Government, and no official endorsement should be inferred.

References and recommended reading

Papers of particular interest, published within the period of review, have been highlighted as:

- • of special interest
- •• of outstanding interest

1. Acquisti A, John LK, Loewenstein G: **What is privacy worth?** *J Leg Stud Educ* 2013, **42**:249-274.

2. Goffman E: *The Presentation of Self in Everyday Life*. New York: Anchor Books; 1958.

3. Gharib S: **Intel CEO says data is the new oil**. *Fortune*. 2018 . Retrieved from *http://fortune.com/2018/06/07/intel-ceo-brian-krzanich-data/*.

4. Kim T, Barasz K, John LK: **Why am I seeing this ad? The effect of ad transparency on ad effectiveness**. *J Consum Res* 2018, **45**:906-932.

5. Steel E, Locke C, Cadman E, Freese B: *How Much is Your Personal Data Worth?* . Retrieved from: Financial Times; 2013 *https://ig.ft.com/how-much-is-your-personal-data-worth/*.

6. Dietvorst BJ, Simmons JP, Massey C: **Algorithm aversion: people erroneously avoid algorithms after seeing them err**. *J Exp Psychol Gen* 2015, **144**:114-126.

7. • Dietvorst BJ, Simmons JP, Massey C: **Overcoming algorithm aversion: people will use imperfect algorithms if they can (Even slightly) modify them**. *Manag Sci* 2016, **64**:1155-1170

In this study, the authors demonstrate that people are substantially more comfortable with algorithms when they are able to slightly modify them. While in the context of recommendations, this research is clearly applicable to people's interactions with algorithmic privacy options as well.

8. Jago AS: **Algorithms and authenticity**. *Acad Manag Discov* 2019, **5**:38-56.

9. • Logg JM, Minson JA, Moore DA: **Algorithm appreciation: people prefer algorithmic to human judgment**. *Organ Behav Hum Decis Process* 2019, **151**:90-103

Here, the authors explore when and why people choose to rely on algorithmic advice. They find evidence that people are generally more comfortable with algorithms than previous research would suggest.

10. Kramer AD, Guillory JE, Hancock JT: **Experimental evidence of massive-scale emotional contagion through social networks**. *Proc Natl Acad Sci U S A* 2014, **111**:8788-8790.

11. Newman D, Fast NJ, Harmon DJ: *When Eliminating Bias isn't Fair: Algorithmic Reductionism and Procedural Justice in Human Resource Decisions*. . Unpublished manuscript University of Southern California; 2019

This paper presents evidence suggesting that those being evaluated by HR algorithms perceive the process as reductionistic, leading them to think that certain qualitative factors or contextualizations are not being taken into account. The authors argue that this can undermine the perceived procedural fairness of using HR algorithms to evaluate performance by fostering the assumption that algorithm-based decisions are based on less accurate information than identical decisions made by humans.

12. James G, Witten D, Hastie T, Tibshirani R: *An Introduction to Statistical Learning: With Applications in R*. New York: Springer; 2013, 15-28:. 112.

13. Larson J, Mattu S, Kirchner L, Angwin J: *How We Analyzed the COMPAS Recidivism Algorithm*. ProPublica; 2016 Retrieved from: *https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm*.

14. •• Wang Y, Kosinski M: **Deep neural networks are more accurate than humans at detecting sexual orientation from facial images**. *J Pers Soc Psychol* 2018, **114**:246-257

The authors demonstrate that a machine-learning algorithm outperforms people when detecting sexual orientation using faces. This article serves as an important milestone in understanding the extent to which algorithms will be able to autonomously invade privacy.

15. Whalen v. Roe: 429 U.S. 589; 1977.

16. John LK: **The consumer psychology of online privacy: insights and opportunities from behavioral design theory**. In *The Cambridge Handbook of Consumer Psychology*. Edited by Norton MI, Rucker DD, Lamberton C. Cambridge University Press; 2016:619-646.

17. Fointiat V: **Rationalization in act and problematic behavior justification**. *Eur J Soc Psychol* 1998, **28**:471-474.

18. Johnson RE: **Smoking and the reduction of cognitive dissonance**. *J Pers Soc Psychol* 1968, **9**:260-265.

19. Kunda Z: **The case for motivated reasoning**. *Psychol Bull* 1990, **108**:480-498.

20. Jenni K, Loewenstein G: **Explaining the identifiable victim effect**. *J Risk Uncertainty* 1997, **14**:235-257.

21. Downes L: **GDPR and the end of the internet's grand bargain**. *Harv Bus Rev* 2018 . Retrieved from: *https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain*.

22. Lucas G, Gratch J, King A, Morency LP: **It's only a computer: virtual humans increase willingness to disclose**. *Comput Hum Behav* 2014, **37**:94-100.

23. Raveendhran R, Fast NJ: **Technology and social evaluation: implications for individuals and organizations**. In *The Cambridge Handbook of Technology and Employee Behavior*. Edited by Landers RN. Cambridge University Press; 2019

The authors argue and provide support for the idea that that interacting with technology and humans is a different psychological experience, even when the task and objectives are the same. People experience higher social evaluation concern when interacting with humans and interacting with technology alleviates these concerns.

24. Raveendhran R, Fast NJ: *Humans Judge, Algorithms Nudge: When and Why People Embrace Behavior Tracking*. . Unpublished manuscript University of Southern California; 2019.

25. Benlian A, Klumpe J, Hinz O: **Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: a multimethod investigation**.. Forthcoming *Inf Syst J* 2019. in press.

26. Waytz A, Heafner J, Epley N: **The mind in the machine: anthropomorphism increases trust in an autonomous vehicle**. *J Exp Soc Psychol* 2014, **52**:113-117.

27. Staw BM: **The escalation of commitment to a course of action**. *Acad Manag Rev* 1981, **6**:577-587.

28. Kanter J: *The Backlash That Never Happened: New Data Shows People Actually Increased Their Facebook Usage After the Cambridge Analytica Scandal*. . Retrieved from: 2018 *https://www.businessinsider.com/people-increased-facebook-usage-after-cambridge-analytica-scandal-2018-5*.

29. Mirhaydari A: *Facebook Stock Recovers All $134B Lost After Cambridge Analytica Data Scandal*. . Retrieved from: 2018 *https://www.cbsnews.com/news/facebook-stock-price-recovers-all-134-billion-lost-in-after-cambridge-analytica-datascandal/*.

30. Festinger L: *A Theory of Cognitive Dissonance*. Palo Alto, CA: Stanford University Press; 1957.

31. • Laurin K: **Inaugurating rationalization: three field studies find increased rationalization when anticipated realities become current**. *Psychol Sci* 2018, **29**:493-495
Here, the author demonstrates that something unpleasant actually happening encourages rationalization by virtue of those negative things feeling more psychologically 'real'.

32. Laurin K, Kay AC, Fitzsimons GJ: **Reactance versus rationalization: divergent responses to policies that constrain freedom**. *Psychol Sci* 2012, **23**:205-209.

33. Laurin K, Kay AC, Proudfoot D, Fitzsimons GJ: **Response to restrictive policies: reconciling system justification and psychological reactance**. *Organ Behav Hum Decis Process* 2013, **122**:152-162.

34. Brynjolfsson E, McAfee A: *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W.W. Norton; 2014.

35. Hiroto DS, Seligman ME: **Generality of learned helplessness in man**. *J Pers Soc Psychol* 1975, **31**:311-327.

36. Kummer M, Schulte P: **When private information settles the bill: money and privacy in Google's market for smartphone applications**. *Manag Sci*; in press. Retrieved from: https://doi.org/10.1287/mnsc.2018.3132.

37. Schwartz B: **The social psychology of privacy**. *Am J Sociol* 1968, **73.6**:741-752.

38. Tversky A, Kahneman D: **Availability: A heuristic for judging frequency and probability**. *Cogn Psychol* 1973, **5(2)**:207-232.