Jeremy Pitt

Complacency is the New Normal

Shifting Public Discourse on Technological Acceptability

One definition of paranoia is as a symptom of a clinically-diagnosed mental disorder, from which a sufferer believes that others are attempting to cause them harm. The term "paranoia" also has a colloquial meaning, used to describe an individual who is excessively, "obsessively," or unreasonably anxious or mistrustful of the motives of other people or organizations, in particular feeling that those people or organizations are "out to get them." Without wishing to underestimate the seriousness of mental conditions, or the distress that they causes both sufferers and those near to them, this article is going to use the terms *paranoia* and *paranoid* in their colloquial sense.

It has been suggested that, in order to maximize throughput, minimize delays, and treat all data traffic equally, there is a lack of memory, structure, and regulation in the technical layers of the Internet (i.e., network and transport layers). In conjunction with "network effects" (the network becomes more valuable as the number of nodes increases), this lack of structure has enabled the centralization of control and the economic dominance at the application layer [1]. As a result, a small number of technology giants ("tech giants") have emerged. Each of these is a private trans-national company dominating (sometimes almost to the point of monopoly) a domain of enterprise on the Internet (e.g., search: Google; e-commerce: Amazon; transportation: Uber; social networking: Facebook; etc.)

For the sake of argument (and with apologies to Pascal [2]), let us suppose there is a tech giant, called DayterGrabbas. The actual service or product provided by DayterGrabbas is irrelevant here, but suppose also that to access the service requires that users must provide significant and substantial amounts of personal data [3]. DayterGrabbers could therefore exploit their (dominant) network position in a number of ways: either through taking ownership of personal data and/or control of data flows, uniquely identifying individuals, invading individuals' privacy, or enjoying an asymmetric distribution of the benefits (and power relationship) that are accrued.

DayterGrabbas includes the clause "Don't do Evil" in its employees' Code of Conduct; but it is not entirely clear why it is there, or if the company really means it or not.[1] Neither reason, nor recommendation, nor reassurance are enough to decide which of the two alternatives (doing evil or not doing evil) DayterGrabbas will actually pursue.[2]

A toss of the coin is going to be made, where heads or tails will definitely turn up. In other words, DayterGrabbas will either definitely do evil, or it will definitely not do evil.

Now each and every user *must* make a separate call on the toss of a coin (participation is not optional). In other words, the only alternative to not using the service or product offered by DayterGrabbas is the 21st century's socio-technological equivalent of being a medieval hermit, living in a cave and eating air.

So each user's options are: s/he should be paranoid (in the colloquial sense of the term), and believe that DayterGrabbas is planning to do evil with your (and everyone else's) data; or there is no need to be paranoid, and believe that DayterGrabbas is not planning to do evil.

Then consider the gains and losses in betting that s/he should

---

[1] It would not be unreasonable, of course, to inquire why the organization should need such an injunction against doing evil in the first place: an expectation that this is the default mindset of its employees? A thin veneer of virtue to gain competitive advantage over rival organizations, with little or no real intent? Expressing a genuine distancing from business practices that are based on an asymmetric and exploitative relationship between platform owners and data aggregators on the one hand, and their users on the other? A prescient awareness of the potential for its technology to be weaponized for military applications of debatable ethical standing?

[2] Pure coincidence of course, but tech giant Google did once include the clause "Don't be Evil" in its corporate Code of Conduct from 2000, which seems to have been displaced in 2018 [4].

Digital Object Identifier 10.1109/MTS.2018.2876101
Date of publication: 30 November 2018

be paranoid. If s/he is paranoid, and DayterGrabbas is planning to do evil, then s/he retains existing practices and protections regarding data, identity, and privacy. But if s/he is paranoid, and DayterGrabbas is not planning to do evil, then s/he has lost nothing by the investment in securing these items. Clearly, if the user does not share, there would be a cost in terms of not getting personalized service, or not getting the benefits of an aggregated service. However, if the user does share, then it does not mean that s/he has to sacrifice data ownership, identity and, privacy (if for example DayterGrabbas committed to only collecting data that is necessary and keeping it for as long as warranted; were not able to identify individuals from aggregated data; and would not pass or sell data to unspecified third parties), or tolerate an asymmetric distribution of rewards (and power) between DayterGrabbas and its user base.

Consider, alternatively the gains and losses in betting that the user should not be paranoid. If s/he not paranoid, and DayterGrabbas is not planning to do evil, then s/he has gained nothing. But if s/he is not paranoid, and DayterGrabbas is planning to do evil, then s/he loses everything: data, identity, and privacy. Moreover, this might even be the thin end of a large wedge, if unscrupulous manipulation of the service undermines other values (e.g., the very concept of liberal democracy itself [5]) or can be weaponized without democratic oversight.

This implies that if a user configures all the available privacy options to the most paranoid, then s/he retains control over his/her own data, identity, and privacy if DayterGrabbas plans to do evil, but if not, s/he would be no worse off than if s/he had not configured them. On the other hand, if the user did not care and did nothing, then depending on whether DayterGrabbas is or is not planning to do evil, s/he either gains nothing or loses everything. The user is either blissfully ignorant (if DayterGrabbas is not planning to do evil, then (in principle) nothing needs to be done about data ownership, identity, and privacy) — or the user sacrifices data control, privacy, and identity on the altar of DayterGrabbas' pursuit of world domination, or to a libertarian society advocating "small government" and private ownership of public infrastructure and natural resources (conveniently overlooking that DayterGrabbas was founded using support from a government grant, and its business model is completely dependent on a infrastructure built largely with public money and collective academic action).

Therefore, the logical conclusion would be that it is "safer" to be "paranoid." Of course, that is the conclusion, since the argument has been set up to be structurally identical to Pascal's Wager, where on the basis of the same set of premises he reaches the logical conclusion that it is "safer" to believe in God than not.

However, there is one substantive difference and one significant similarity between Pascal's Wager and the "paranoia version" presented here. Regarding the substantive difference, each person taking Pascal's Wager and choosing not to believe in God would not materially affect any other person taking the Wager irrespective of the choice that they make. However, each person taking the wager of the paranoia version and choosing not to be paranoid *does* materially affect others. This is partly because of the network effects mentioned above, but also partly because of "no man is an island entire unto himself." A diminution of one person's individual identity or privacy is eventually a diminution of everyone's; and it can have subtler, longer-term pernicious side effects on social cohesion, a sense of community, and opportunities for collective action. Individuals not "on" certain dominant social media platforms can face difficulty in creating accounts with other services; can find themselves being tagged and tracked even though they never even opted in; and can even encounter a kind of social exclusion that is the near equivalent of "living in a cave" after all. Furthermore, the aggregation of enough individuals' data is enough to effectively identify us all, such is the mathematical inevitability of logistic regression combined with the unfortunate fact that, in general, people are not nearly as unique as they would like to think that they are [6].

Regarding the significant similarity, the wager has an impact on both popular culture and public discourse. In particular, the choice can affect what is, and is not, acceptable to say in public, but also how those, especially those in a minority, are perceived and portrayed in popular culture. Indeed, the *Overton Window* has been defined as the "range of ideas tolerated in public discourse… an idea's political viability depends mainly on whether it falls within the window, rather than on politicians' individual preferences." Consciously attempting to shift the window can be seen in operation in the statements of any politician who claims "You can't say this but …" and then goes on to say exactly what, apparently, cannot be said.

It would seem though that the Overton Window also applies to technological, as well as political, acceptability. The giant trick involves two steps. The first step has been to shift intrusions into privacy and the aggregation of data into the realm of the acceptable by associating those who have concerns about it with being paranoid. For example, one Internet search (to repeat this, use a search engine of one's choice; depending on which organization you want to allow to have this information, the search might yield different results) using the terms "online privacy paranoia" yields articles with the following titles:

- Are You Too Paranoid About Your Digital Privacy?
- 13 Security and Privacy Tips for the Truly Paranoid
- When it comes to online security, being paranoid is no longer enough
- How to escape the online spies
- How paranoid is too paranoid when it comes to privacy and security?
- Now What? Protecting Online Privacy in An Age of Paranoia
- Internet privacy: Genuine concerns or paranoia?
- 5 secure habits of the paranoid PC user
- The Paranoid Conspiracy-Theorist's Guide To Online Privacy & Security
- 8 Tools for the Online Privacy Paranoid

Repeating the search with "not paranoid" as the search term rather than "paranoia" yields some different articles. However the new results all still manifest the same underlying assumption: genuine, reasonable concerns over online privacy are labeled as paranoia. Apparently, unless you are paranoid, it really is ok to have a microphone in your kitchen, in your television, and on your portable device. What could possibly go wrong?

The second step is to rely on the cultural perception that paranoia has *negative* rather than positive connotations and that anyone exhibiting such "paranoia" can be effectively dismissed, as per its colloquial definition, as obsessive, unwarranted, delusional, and exaggerated. Unfortunately, of course, but for the sake of making a point, the "paranoia version" of Pascal's Wager presented here is effectively buying into the same frame and the same central conceit. However, it needs not to be forgotten and perhaps more than ever needs to be emphasized:

> *What is now "paranoia" is actually the old "normal."*

The level of state surveillance practiced in the supposedly illiberal regimes prior to fall of the Berlin Wall is now routinely accepted, from the widespread use of CCTV to online tracking and data recording. Therefore, instead of labeling a display of genuine concern as "paranoia," perhaps a lack of genuine concerns should instead be stigmatized by a "disease" or a "disorder": complacentosis, complyaphilia, complicivitis, ignorrhea.

This is not to deny that many, perhaps most, of us are sufferers, at least to some extent. But a number of the articles in this issue can be construed as addressing the potential risks (and, to be fair, potential rewards) of several emerging technologies. These risks and potential rewards include Artificial Intelligence, virtual reality, and robotic olfaction. The review of the re-release of Mary Shelley's Frankenstein prompts recollection of the principle of unintended consequences and the importance of the precautionary principle. It should remind, perhaps even shame, those of us who have not had to fight so much or so hard for rights, or representation, or even for personal safety in a failing state, how we have so glibly, even willingly, been prepared to surrender such hard-won values for the sake of the latest gadget or fangled technology. It is *not* paranoid to have concerns, it is instead our civic responsibility, a legacy of campaigners from Tom Paine onwards. It is critical that the window of public discourse is shifted back to reflect that responsibility.

Editor's Note

I am grateful to Marcello D'Agostino for first pointing out to me the logical similarity between believing in a deity and opting for paranoia, Simon Dobson for introducing me to the Overton Window, and Ada Diaconescu for the observation regarding the inversion of "normal" and "paranoid." However, opinions expressed in this article are those of the author and not necessarily shared by these individuals.

It is also a great pleasure to welcome as Associate Editors Greg O'Hare (University College Dublin, Ireland), Steve Marsh (University of Ontario Institute of Technology, Canada), Kristina Milanovic (Imperial College London, U.K.), and Joe Carvalko, Quinnipiac University. Thank you in advance for your contributions to Technology and Society Magazine.

Author Information

Jeremy Pitt is Professor of Intelligent and Self-Organizing Systems at Imperial College London, U.K. Email: j.pitt@imperial.ac.uk.

References

[1] Special Report, "The story of the internet is all about layers," *The Economist*, June 2018; https://www.economist.com/special-report/2018/06/28/the-story-of-the-internet-is-all-about-layers.

[2] A. Hajek, "Pascal's Wager." *Stanford Encyclopedia of Philosophy*, 2017; https://plato.stanford.edu/entries/pascal-wager/.

[3] J. Wernimont and N. Stevens, "Seeing 21st century data bleed through the 15th century Wound Man," *IEEE Technology & Society Mag.*, this issue.

[4] K. Conger, "Google removes "Don't Be Evil" clause from its Code of Conduct," *Gizmodo*, May 2018; https://gizmodo.com/google-removes-nearly-all-mentions-of-dont-be-evil-from-1826153393.

[5] C. Cadwalladr, "Electoral law has been broken — This is a fight for the soul of our democracy," *The Observer*, July 2018; https://www.theguardian.com/politics/2018/jul/08/electoral-law-broken-fight-for-soul-of-democracy.

[6] O. Burkeman, "Think you're special? That just proves you're normal," *The Guardian*, May 2018; https://www.theguardian.com/lifeandstyle/2018/may/04/think-special-just-proves-you-are-normal.