Kirsten McNally (2021) *'Accept All'. How Hyperbolic Discounting Renders PSM a Faulty Foundation for Privacy Protection.*, Studies in Philosophy, Politics and Economics, 3(1), 38-43

Studies in Philosophy Politics and Economics

'Accept All'. How Hyperbolic Discounting Renders Privacy Self-Management a Faulty Foundation for Privacy Protection

Kirsten McNally [1]

[1]Philosophy, Logic and Scientific Method, London School of Economics, Houghton Street, London, WC2A 2AE, UK. Email: kirsten.mcnally@icloud.com. URL: www.linkedin.com/in/kirsten-mcnally-287173166

Abstract

Regarding the legal rules concerning the processing of personal data, Solove proposes that Privacy Self-Management (PSM) is undermined by cognitive and structural problems, meaning its reliance on consent is flawed (Solove 2013). I agree with his argument, specifically concerning cognitive problems, and extend this to the issue that humans choose smaller, immediate rewards rather than larger, later rewards, which is damaging to the status of the consent transaction. I then argue that this cognitive problem is worsened by the Internet environment. The use of default settings, enabling minimal data revelation, established by an independent body is then discussed as a solution.

Keywords: PSM; Data Privacy; Consent.

Privacy Self-Management (PSM) describes the rights giving users control over collection and usage of their data, based on given consent, meaning the processing of personal data is permitted where consent is explicitly granted by the data subject (Solove 2013). This paradigm underlies existing data protection laws, including the European Union's 2018 General Data Protection Regulation (GDPR). Under GDPR Article 6, the provision of consent is a sufficient condition for the lawful processing of data (GDPR.EU 2020). If Internet users can provide it, unambiguous, informed, voluntary consent is seemingly an excellent benchmark for establishing legal rules governing data processing as it purportedly grants normative sanction to an act or outcome that would not be permitted absent consent (Kleinig 2009). However, I agree with Solove that PSM is unsuitable for determining the legal rules governing the processing of personal data, as its reliance on the normative power of consent ignores the cognitive problems faced by those granting it. I assume that legal rules should settle disputes and protect individuals from harm (Waldron 2020), and whilst PSM may settle disputes, legal rules based on PSM fail to protect individuals from harm.

LSE Houghton St Press

PSM is unsuitable for determining legal rules governing data processing due to cognitive problems (Solove 2013). Solove describes decision-making as being skewed by cognitive hurdles including the framing of choices and faulty risk assessment but does not discuss in detail how cognitive hurdles can lead people to act against their true preferences. One such cognitive hurdle is hyperbolic discounting, which is one example of how preferences can be dynamically inconsistent. Adapting Laibson's example of saving choices (Laibson 1997) to consenting to data processing, hyperbolically discounting Internet users with a desire for privacy protection in the long-term click 'Agree' to a site's request to process their data in the current moment, rather than clicking 'More Options', with the intention that they will make the choice which is consistent with a long-term preference for data protection next time. However, the next time the request to process data pops up, they again click 'Agree'. Each time they are faced with the decision, they choose to postpone the time-consuming activity and instead choose to accepting data processing, which is not in their long-term interests of data privacy. Rather than postponing a hit to their current budget, as in Laibson's example, they are postponing a sacrifice of time. For Internet users, the future is not discounted at a constant rate. In two weeks, the difference in their utility between changing privacy preferences, rather than consenting, on Tuesday rather than Monday is negligible. However, when scrolling the Internet today, there is significant utility difference between pushing back this task until tomorrow and disrupting current browsing to fix it immediately. If some individuals do know that 'Accept' affords lesser protection of data than restricting data processing, yet still select it at each present moment, the user prefers instant gratification to long-term privacy protection, even though at other times they prefer the reverse.

The foregoing aligns with the inconsistencies between stated privacy preferences, and protection of it. People ardently defend their right to privacy over their sexual orientation and politics, yet 48% and 47% shared information on these topics respectively. Though not definitive, present bias (characteristic of hyperbolic discounting) is posited as a cause (Acquisti et al. 2015: 510). Clearly, some users will misunderstand the consequences of their acceptance and so cannot be characterized as making an informed trade-off between accepting data processing and protecting long-term privacy. However, the uninformed user still chooses to gratify their current desire to use the Internet, over *becoming* informed by considering 'More Options' and so could still be viewed as a hyperbolic discounter; at each present moment they would rather not spend time learning about their options, leading to consent to data processing through a time-saving click of 'Accept'. The acceptance in both cases provides the condition needed for sites to process personal data. For example, users consent for personal data to be processed by a website, which permits Google to use their data to 'improve' services (Google 2020). This results in targeted adverts appearing in future, potentially creating harm by inducing purchases, creating a sense of privacy invasion against a stated preference for privacy, or increasing the risk of a data breach for the individual. Individuals must weigh this against decreased search costs and improved Internet experience in a rational decision-making scenario, yet as described, the decision to consent is not born out of this cost-benefit analysis. Cambridge Analytica, a data analysis firm, was in breach of Facebook's own rules when harvesting personal data for use in targeted political advertising, after a Facebook policy change in 2015 (Romm 2020), but it is conceivable that Facebook users would consent to this processing of personal data to gratify immediate scrolling, without considering the future potential consequences of targeted political adverts, simply by not checking their preferences. Information disclosure through consent gratifies users' current selves, whilst exposing their future selves to privacy costs, with users' hyperbolic discounting encouraging the initial consent (Acquisti et al. 2015). Consent may therefore not be a true expression of preferences against potential harm, making it unsuitable for determining legal rules for data processing.

The tedious nature of considering data processing online only worsens the tendency to hyperbolically discount. An amusing example of this is a study of students' willingness to agree to Privacy Policies and Terms of Service. 98% of those studied accepted terms which they simply had not read, and which gave explicit consent for a (fictitious) social networking site to take their first-born child as payment for site access (Obar and Oeldorf-Hirsch 2020). Whilst of course regulations would prohibit this, there are unsettling real-world Terms of Service. For example, Twitter reserves the right to sell a picture of your family, or any image uploaded, universally, with no compensation to you (Twitter 2021). Obar & Oeldorf-Hirsch present acceptance as resulting from 'information overload' (2020: 23). Hyperbolic discounting may be important here, as what is perceived by our current selves as 'information overload' may be perceived as an important document to read for our future self who values privacy protection. The opportunity cost of reading is admittedly significant for an individual wanting to use the Internet, given that the median reading time for one full policy is ten minutes (McDonald and Cranor 2008: 554). The user must weigh this significant cost to their present selves against the benefit of ignoring it and blindly consenting, perhaps promising that they will read it next time, which is arguably a reasonable response, given the time this would save. However, hyperbolic discounting causes a saved ten minutes from not reading the policy to be judged as having even greater benefit than avoiding the harm to long-term privacy preferences. This harm to privacy might be significant as ignored 'Terms of Service' accumulate across sites, leading to 'cookie profiling' where an aggregated picture of online activity is generated, which some view as useful, but others see as a salient example of privacy invasion (Geary 2021). The cost-benefit analysis does not appear to account for the prevention of this harm. Giving consent has become akin to minimizing a popup, with individuals simply consenting 'whenever confronted with a consent request' (Schermer et al. 2014: 171). Arguably this is a genuine expression that the Terms of Service are unimportant or that the lost time from reading them genuinely not worth it. However, this is inconsistent with the strong preferences that individuals express for privacy, which reviewing Terms of Service should allow protection of. Although perhaps not the sole explanation for this contradictory behaviour, I find hyperbolic discounting to be a compelling one. This is a difficult cognitive fault to overcome. Neither improved information nor improved usability, such as more user-friendly language in Terms of Service, target the issue that users' simply value the utility of their current selves more than the utility of their future selves, leading them to simply ignore Terms of Service, jeopardizing their future selves' preference for privacy.

Given that hyperbolic discounting is a difficult cognitive problem to overcome, as improved Terms of Service may still be ignored, one potential solution is the use of defaults. Through defaults, individuals could be steered towards decisions that are optimal for them, with the possibility of opting out, should they actively engage in cost-benefit analysis and express their true preferences against the default. In the online environment, the default will be defined as the data processing mechanisms that a website uses, without requiring active clicking of sliders or tick boxes by the user, as is currently the case. Considering social media, default user settings have often been found to lend themselves to high levels of information revelation, which is potentially not optimal for the individual (Acquisti et al. 2017). Rather than asking every user if they 'Accept' data processing, the default setting on a site should be legally set to a level of data processing which protects the individual from harm of privacy invasion. Though vulnerable to criticisms of paternalism, if consumers do not have well-formed preferences over their privacy due to hyperbolic discounting, defaults may be a valid form of protection (Johnson et al. 2002). Paternalism is sometimes criticised on the grounds that users know their preferences best. However, defaults may also be justified if many do not understand the consequences of interactions in this environment, such that there is a responsibility to establish a protective default setting which disengaged or confused users can resort to.

The use of defaults has been effective in pension saving, an area where hyperbolic discounting is well-documented. If consumers knew their preferences best, auto-enrolment in pensions should not affect saving decisions, as they would already be saving at their optimal level, yet studies suggest that it has increased pension participation (Choi et al. 2004). Moreover, auto-enrolment means many save at the default contribution rate imposed at auto-enrolment. By increasing auto-enrolment savings rates, savings increased, as most passively accepted the increases (Choi et al. 2004). Households identified as under-saving revealed that they wanted to save more and so their individual well-being should have increased through being subjected to a higher default savings rate (Thaler & Benartzi 2001 in Choi et al. 2004).

Although the problem faced by the Internet user is different, with the hyperbolic discounter postponing a time sacrifice with future privacy, rather than saving with consumption, Internet users may also benefit from improved quality of ‘default’ options. Perhaps an independent body such as the Information Commissioner’s Office (ICO) could establish defaults to be at the minimal level of data revelation needed for free sites to continue operation, whilst maximising data protection. Currently, the ICO acts against breaches in data protection policy, but it could be given a more proactive role in the protection of Internet users. This would mirror the approach adopted in the UK regarding pension schemes when the Financial Cconduct Authority mandated the introduction of Independent Governance Committees in any workplace offering workplace pensions, which could oversee the default funds employee pensions used (Financial Conduct Authority 2019). The establishment of this minimal level would be contentious, given financial interests. However, personalized defaults set by system designers have been suggested, catering for the range of understanding across Internet users with customization available for more advanced users to meet more advanced needs (Acquisti, et al. 2017: 21). Rather than leaving these choices to the technology industry’s system designers, we could hand design responsibility to an independent body whose aims align with data protection rather than data harvesting, to protect long-term preferences for data privacy.

In conclusion, Solove correctly identifies cognitive flaws as barrier in using PSM to guide legal rules for data processing but I have argued that specifically, it is users’ tendency to hyperbolically discount which renders consent a faulty foundation for legal rules, which is worsened by the Internet environment. An alternative should be sought such that cognitive impairments do not leave users susceptible to harm. I have suggested that defaults could be used to provide higher minimal standards for data processing requirements.

References

Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L.F. Cranor, S. Komanduri, P.G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang and S. Wilson. 2017. Nudges for privacy and security: understanding and assisting users' choices online." *ACM Computing Surveys* 50 (3): 1--41.

Acquisti, A., L. Brandimarte and G. Loewenstein. 2015. Privacy and human behaviour in the age of information. *Science* 347: 509--514.

Choi, J.J., D. Laibson, B.C. Mandrian and A. Metrick. 2004. For better or for worse: default effects and 401(k) savings behavior. *Perspectives on the Economics of Aging*, ed. D. Wise, 81--121. Chicago: Chicago University Press.

Financial Conduct Authority. 2019. Independent Governance Committees*. Financial Conduct Authority Web Site.* URL: https://www.fca.org.uk/firms/independent-governance-committees

GDPR.EU. 2020. What is GDPR, the EU's new data protection law? *GDPR.EU Web Site*. URL: https://gdpr.eu/what-is-gdpr/

Geary, J. 2021. Tracking the trackers: What are cookies? An introduction to web tracking*. The Guardian.* URL: https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro

Google. 2020. How google uses information from sites or apps that use our services*. Google Privacy & Terms.* URL: https://policies.google.com/technologies/partner-sites?hl=en-US

Johnson, E.J., S. Bellman and G.L. Lohse. 2002. Defaults, framing and privacy: why opting in-opting out. *Marketing Letters* 13: 5--15.

Kleinig, J. 2009. The Nature of Consent. In *The Ethics of Consent: Theory and Practice*, ed. F.G. Miller and A. Wertheimer. 3--24. Oxford: Oxford University Press.

Laibson, D. 1997. Golden eggs and hyperbolic discounting. *Quarterly Journal of Economics* 112: 443--477.

McDonald, A.C. and L.F. Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4: 543--568.

Obar, J.A. and A. Oeldorf-Hirsch. 2020. The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23: 128--147.

Romm, T. 2020. Facebook will have to pay a record-breaking fine for violating users' privacy. But the FTC wanted more*. The Washington Post.* URL: https://www.washingtonpost.com/technology/2019/07/22/facebook-vs-feds-inside-story-multi-billion-dollar-tech-giants-privacy-war-with-washington/

Schermer, B.W, B. Custers and S. van der Hof. 2014. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology* 16: 171--182.

Solove, D.J. 2013. Privacy self-management and the consent dilemma. *Harvard Law Review* 126: 1880--1904.

Thaler, R.H. and S. Benartzi. 2001. Save More Tomorrow™: using behavioral economics to increase employee saving. *Journal of Political Economy* 112: 164--187.

Twitter. 2021. *Twitter Terms of Service.* URL: https://twitter.com/en/tos

Waldron, J. 2020. The Rule of Law. *Stanford Encyclopedia of Philosophy (Summer 2020 Edition)*. E.N. Zalta (ed.), URL: https://plato.stanford.edu/archives/sum2020/entries/rule-of-law/