The Professor Maureen Brunt AO Essay Prize

Paying for privacy: An exploration of the trade of personal information and privacy in the digital age. Human right? Property right? Input to production?

Essay Title: The privacy catch-22: how current information privacy norms position individuals with the responsibility but not the power

Essay Word Count: 2931

Essay Type: Persuasive

Abstract:

Current privacy rhetoric, including the information privacy legal landscape, has not fully accounted for growing power asymmetries between those who generate data, and those who use it. In this essay I argue that current privacy norms simultaneously position individuals as key actors with control over their privacy, while upholding a complex system in which consumers are not actually able to exercise meaningful control over flows of information. Through an examination of some of the key tenets of information privacy including the definition of 'personal information,' the consent-based model and emphasis on transparency of data practises, the essay posits that these well-intentioned concepts are no longer effective at serving the interests of consumers in the digital age. This is exacerbated by the 'trade-off' narrative which creates a false choice between technology and privacy, due to the belief that technology is inherently privacy-invasive. While individual autonomy and control will always be an important part of the information privacy dialogue, the status quo is unfair on consumers. It is time to shift the responsibility onto those who hold the power (and the data), to instil fair, ethical data practices, instead of offloading responsibility onto individuals.

The privacy catch-22: how current information privacy norms position individuals with the responsibility but not the power

It is not an overstatement to say that technology is "embedded in the most intimate and most mundane" parts of modern life.[1] Each time we access government services, make a transaction, build communities online or even just walk down the street, data is being created, collected, used and shared. This

[1] Sarah Myers West, "Data Capitalism: Redefining the Logics of Surveillance and Privacy," *Business and Society*, Vol 58(1) (2019): 21.

phenomena is well known, to the extent that it is considered an inherent part of using technology; we are told this is the price we pay for access to products and services. This essay argues that current privacy norms simultaneously position individuals as key actors with control over their privacy, while upholding a complex system in which consumers are not actually able to exercise meaningful control over flows of information. The catch-22 of placing the burden of responsibility onto individuals while upholding a system they have no power in, is comparable to convincing people they can make a meaningful impact on climate change by boycotting the use of plastic straws. Privacy is not simply an individual problem. It is also a structural one.

Much of information privacy discourse has not accounted for the growing power asymmetries between institutions that accumulate data, and the individuals who generate it.[2] Treating data as a tradable good does not acknowledge the difficulty for people to make privacy-related decisions when dealing with systems they do not understand, particularly when the system has learnt, by way of ingesting their data, how to manipulate their preferences. Under a system of surveillance capitalism in which data is treated like currency, power has been weighted towards those who have access and ability to make sense of the data. This essay first examines how some of the key tenets of information privacy such as the definition of 'personal information,' consent-models and transparency have been transformed to no longer serve the interest of consumers in the digital age. The 'trade-off' rhetoric is then critiqued, arguing that consumers are faced with a false choice due to the narrative of privacy erosion being an inevitable part of technological advancement. By scrutinizing the status quo of information privacy norms, it is clear that the current emphasis placed on individual autonomy is neither a reflection of reality, nor an effective method of protecting privacy. If information privacy is to be anything more than a tick-box exercise as we progress further into the digital age, the weight of responsibility needs to be shifted onto those who hold the power, rather than superficially given to individuals who in reality have very little ability to make meaningful choices about their privacy.

While often dismissed as the area for the luddites and the paranoid, questions of information privacy are some of the most important we face in the digital age. Beyond its value as a human right, privacy also holds immense value in its role in upholding other rights and freedoms.[3] Intricately linked with ethical use and processing of data, information privacy serves as an important litmus test for many technological advancements including Internet of Things (IoT) devices collecting data in previously unimaginable ways, and widespread adoption of quickly evolving artificial intelligence techniques. We have already seen a glimpse into a world in which ethical data handling and privacy is not taken seriously: the world of Cambridge Analytica and manipulation of democratic processes on a mass scale.

---

[2] Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker and Kate Crawford, "AI Now 2017 Report," *AI Now Institute at New York University* (2017): 28.

[3] International Conference of Data Protection & Privacy Commissioners, "International Resolution on Privacy as a Fundamental Human Right and Precondition for exercising other fundamental rights," *41st International Conference of Data Protection and Privacy Commissioners*, (October 2019): page 2.

The ability for data to be abused and its potential impact on society should not be underestimated. Finally, the use of data is now so ubiquitous and vital to government and business practices, that information privacy is an essential area for legislative reform and broad societal re-education, making it an extremely important area for policymakers and consumers alike.

Privacy is a broad, nuanced area that many have attempted (and struggled) to define.[4] As a non-fixed social construct, the meaning and value of privacy varies between individuals, impacted strongly by age and culture.[5] In terms of the legislative approach to protecting privacy, the Australian *Privacy Act 1988* and six other pieces of state privacy legislation, as well as comparable jurisdictions around the world, focus on information privacy as a subset of the broader concept.[6] Stemming from the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, information privacy emphasises the individual's ability to exercise control when 'trading' their personal information. This is embodied in core privacy pillars such as consent and transparency, which in action manifest in the form of privacy policies, collection notices and terms and conditions (hereby referred to as 'privacy communications').[7]

Information privacy law generally only protects 'personal information.'[8] In Australia, to receive the protections offered by the *Privacy Act 1988*, data needs to fall under a definition which is based on the idea of *identifiability* - whether or not a person's identity can be reasonably ascertained.[9] While this concept may have been effective when it was conceptualised in the 80s, the distinction between what does and doesn't identify individuals does not account for the increasing ability to link and match data, meaning a combination of seemingly innocuous data can *become* personal information.[10] Even 'de-identification'- a popular method of removing personally identifying elements from a dataset so that it no longer legally falls under the definition of personal information (and therefore no longer enjoys the protection of the Privacy Act) - has been shown to be ineffective.[11] Far from just an issue of semantics, the definition of personal information acts as a gatekeeper of privacy protections.

'Personal information' can evolve alongside legal and societal norms. Yet, the most recent change to the definition *decreased* the scope, to the distress of privacy advocates. In the 2015 *Grubb v*

---

[4] Privacy has been described as the control and safeguard of personal information by Alan Westin in his 1967 Privacy and Freedom, or as the protection of personal space and the right to be let alone by Warren and Brandeis in 1890, and as an aspect of dignity, autonomy, and ultimately human freedom by Schoeman, 1992.

[5] danah boyd and Alice E. Marwick, "Social privacy in networked publics: Teen's attitudes, pracices, and strategies," *A decade in internet time: Symposium on the dynamics of the internet and society* (2011).

[6] Graham Greenleaf, "Privacy in Australia," in *Global Privacy Protection: The First Generation*, eds. James Rule & Graham Greenleaf (Cheltenham: Edward Elgar, 2008), 7-11.

[7] 'Information Privacy' is also referred to as 'data privacy' or 'data protection' in jurisdictions outside Australia.

[8] 'Personal information' is the term used in *The Privacy Act 1988* and the *Privacy and Data Protection Act 2014* (Victoria), however is sometimes also referred to as 'Personally Identifiable Information' in other jurisdictions.

[9] The Office of the Australian Information Commissioner (OAIC), "What is personal information," *OAIC Factsheet* (May 2017).

[10] This is related closely to the concept of 'Mosaic Theory' as highlighted in *United States v. Maynard* in 2010.

[11] Chris Culnane, Benjamin IP Rubinstein and Vanessa Teague, "Health data in an open world," *arXiv preprint arXiv* (2017).

Telstra case and subsequent appeal, it was determined that telecommunications metadata is not personal information, as it is not sufficiently *about* an individual.[12] In March 2019, in response to the *Digital Platforms Inquiry* by the Australian Competition and Consumer Commission (ACCC), the Australian Government announced a review of the *Privacy Act*, including potential to amend the definition of personal information "to capture technical data and other online identifiers."[13] While this is a welcome announcement, it remains to be seen how robust the reforms will be, given the lack of support for strong privacy protections the Australian Government has previously demonstrated.[14] Understanding this definition as a gatekeeper is essential in order to fully grasp the larger structural issues faced by information privacy, and is a key area in which policymakers may be able to implement meaningful change. Continuing to draw a line around personal information is not a true reflection of how data is handled in practice, dismisses the reality of how pervasive data collection actually is, and creates confusing messages for consumers which undermines their ability to fully understand the scope of the situation.

Information privacy is also largely underpinned by consent. Taking the APPs as an example, once defined as 'personal,' there are limitations to what organisations may do with that information. However, there is almost always a subclause that permits collection, use or disclosure provided they obtain the individual's consent.[15] As a concept championed in information privacy law around the world, consent is closely linked with the idea of information self-determination, wherein the individual is empowered to make informed choices. Yet, in practice, this can be (and often is) manipulated as a loophole in order for organisations to do what they like with personal information. Popular "consent" mechanisms include long-winded and confusing Terms of Service (ToS), bundled consent in amongst collection notices and confused privacy policies, click wrap agreements, and implied consent unless people opt-out.

In order for consent to be meaningful, it needs to be voluntary, informed, specific, current, and given by someone who has capacity to do so.[16] Given that privacy communications are notoriously long and hard to understand, consumers are often quite literally unable to meet these requirements. A 2008 study found that it would take 76 working days each year for an individual to read every privacy policy of the platforms they use.[17] This is so ridiculous that it has essentially turned privacy policies into a joke. Traditionally, the consent model has relied on the idea of a transaction, usually at points of

[12] Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017), VID 38 of 2016.
[13] Department of Treasury and Finance, "Regulating in the digital age, Government Response and Implementation Roadmap for the Digital Platforms Inquiry," *Australian Government*, (12 December 2019): 6.
[14] Katharine Kemp and Rob Nicholls, "The federal government's response to the ACCC's Digital Platforms Inquiry is a let down," *The Conversation*, 12 December, 2019.
[15] Specifically: to collect sensitive information (3.3(a)) and to disclose it (7.4), to collect from a third party (3.6(a)), for use or disclosure for a purpose that is not the primary purpose (6.1(a)), for direct marketing 7.3(b) and for cross-border disclosure (8.2(b). The *Privacy Act 1988*, Schedule 1, The Australian Privacy Principles.
[16] OAIC, "Chapter B: Key Concepts," in *Australian Privacy Principle Guidelines.*
[17] Aleecia M. McDonald and Lorrie Faith Cranor, "The cost of reading privacy policies," *Isjlp* 4 (2008): 543.

collection, where there are clearly defined moments of exchange of information.[18] The modern equivalent to this is the 'click-wrap' agreement that requires users to click 'I agree' before continuing. Despite being understood as an ineffective means of communication, they continue to be widespread. A 2020 study found 74% of participants completely skip reading any of the privacy communications. Alarmingly, "98% missed 'gotcha clauses' about data sharing with the NSA and employers, and about providing a first-born child as payment for SNS access."[19]

Knowing these kinds of practices do not work and yet continuing to use them as a means to legally collect, use and disclose data flies in the face of "meaningful" consent. Consent models tell consumers that *they* are responsible for making informed choices about the protection of their information, and yet companies and organisations are creating a system in which they know individuals are not able to do so. It is time to consider that the consent-based model in its current form is not effective, and has even been employed in order to *technically* comply with privacy law, while not actually upholding or respecting individuals' privacy.

Acknowledging that there are flaws in the current approach to obtaining consent, there have been some movements to reinvigorate this area. For example, the European Union's General Data Protection Regulation (GDPR) has attempted to address some of the issues by including a need for express consent, prohibition of bundled consent, and a requirement for clear and plain terms and conditions. In Australia, the ACCC Digital Platforms Inquiry recommended stronger consent requirement reforms to follow suit. There is also a small but growing area arguing that consent alone is not enough. Some have argued for relaxing consent requirements around the collection of personal information, and instead advocate for focusing on accountability and ethical use of personal information.[20] Another potential solution, at least in part, is to legislate limits on specific processing of data regardless of the presence of consent. The early iterations of this can be seen in Canada's *Personal Information Protection and Electronic Documents Act 2000* with the inclusions of 'No-Go Zones.'[21] There is also some technical work being done in the area of 'smart data' XACML (eXtensible Access Control Markup Language), essentially tagging data with metadata including individuals' preferences for how it can be used, no matter where it goes.[22] Victorian Information Commissioner Sven Blummel

[18] Office of the Victorian Information Commissioner (OVIC), "To consent and beyond," *blogpost,* (07 January, 2020). https://ovic.vic.gov.au/blog/to-consent-and-beyond-are-no-go-zones-the-next-frontier-part-1/

[19] Jonathan A. Obar, and Anne Oeldorf-Hirsc, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," *Information, Communication & Society* 23, no. 1 (2020).

[20] Fred H. Cate, Peter Cullen, and Victor Mayer-Schönberger. "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines." March 2014.; See also Eloïse Gratton, *Understanding Personal Information: Managing Privacy Risks*, LexisNexis, 2013 which advocates for an approach focusing on the risk of harm, which would have the result of reducing the burden of the notification obligation (and concurrently, the consent obligation).

[21] The Office of the Privacy Commissioner of Canada, "Consent and Privacy," *Discussion paper,* (May 2016): section 2(b).

[22] Siani Pearson and Marco Casassa Mont, "Sticky Policies: An Approach for Managing Privacy across Multiple Parties," *Computer*, vol. 44, no. 9 (September 2011).

uses buildings as a useful analogy: "we don't get asked for consent to walk into a dangerous building - we're simply not allowed...we expect standards and processes to be in place to ensure they're safe."[23] The current consent-model in Australia is broken, and it's time we stop using it as a loophole to allow harmful data practices.

In conjunction with consent, transparency is a key idea of information privacy that has positive intentions, but has been twisted to become a get-out-of-privacy-jail-free card. Transparent communications about data practices is lauded as the gold star by information privacy law and in consumer expectations. Organisations comply with *purpose specification* principles by providing an explanation to consumers about *why* their data is being collected, and what it will be used for - usually through collection notices. While purported to enhance transparency of data practices, the unfortunate reality of privacy communications is that they are often overly-broad 'catch-all' documents, or a muddled confusion between a policy, notice, or ToS in which consent may or may not also be implied. Even under the reforms of the GDPR, European consumers are still faced with similar issues of being bombarded with policy updates, albeit with less use of 'legalese.' As highlighted above, these methods rarely empower consumers. It begs the question: what good is transparency, if the practices behind it are harmful, and companies *know* that no one is actually reading them. Bombarding individuals with too much information is comparable to the legal concept of 'trial by avalanche.' Generally regarded as an unethical practice, the act of providing someone with a vast amount of documents containing masses of often irrelevant or confusing material can indicate an intention to 'wear down' the reader, and/or wanting to cover all bases out of fear of not meeting all obligations.[24] Whether out of fear of not meeting complex legal privacy requirements, or with outright malicious intent, the way many companies and organisations engage with transparency is not serving its purpose.

It is also worth questioning if perhaps people are genuinely consenting to these practices. There is a common perception that people are beginning to care less about privacy. For instance, Mark Zuckerberg indicated he no longer thought privacy was a social norm in 2010. However, the idea that people - particularly younger people, or, 'digital natives' - are becoming less concerned about their privacy does not hold up against research in this space. Boston Consulting Group found for 75% of consumers in most countries, privacy of personal information remains a top issue, and that people aged 18-24 are only slightly less cautious.[25] Similarly, The Pew Research Centre found that 86% of participants had taken steps to remove or mask their digital footprint and 68% believed that current laws were not good enough in protecting privacy.[26]

---

[23] OVIC, "To consent and beyond," 2020.

[24] Australian Law Reform Commission (ALRC), "Managing Discovery: Discovery of Documents in Federal Courts (ALRC Report 115)," *Professional and Ethical Discovery* (April 2011): section 12.25, 'Trolley load litigation.'

[25] John Rose, Christine Barton and Robert Souza, "The Trust Advantage: How to Win with Big Data," *Boston Consulting Group* (November 2013).

[26] Lee Rainie, Sara Kiesler, Ruogu Kang and Mary Madden, "Anonymity, Privacy, and Security Online," *Pew Research Centre* (2013).

That people would express concern about privacy, but continue to contribute their data via the systems they use is often referred to as the 'privacy paradox.'[27] Technological developments such as IoT devices, smartphones and web tracking mean that data is decreasingly being collected in the traditional 'transaction' context wherein people consciously provide their personal information in which most privacy law was based.[28] Participation in these kinds of systems has become part of our 'social infrastructure,' as described by BigTech big wigs like Zuckerberg and Google's Eric Schmidt. Yet, it has been argued that within the landscape of pervasive data collection, individuals actually have no choice but to enter an "unconscionable contract" to allow their data to be used.[29] Research conducted by the Consumer Policy Research Centre highlighted that individuals feel that "data tracking is increasingly inescapable."[30] Looking internationally, the UK Information Commissioner's Office suggests that people may feel resigned to the use of their data because they feel there is no alternative.[31] Sarah Meyers West argues that users are placed in "a double bind, caught between desires for privacy and the ability to form meaningful communities with other users online without opting out of these services."[32] It is no wonder that people say they care about privacy but do not always act on it.

We often talk about privacy in terms of a 'trade-off,' that individuals trade their data, knowingly or not, in order to access services. As highlighted in Shoshana Zuboff's exploration of Surveillance Capitalism, this is considered a technological necessity, an *inevitable* byproduct of the services and platforms we have grown dependent on (and addicted to, thanks to manipulative design practices).[33] It is important to note, however, that the pivot made by Google in the early 2000s to begin to collect and use the behavioural data it had access to, was less about technological necessity, and more about commercial gain.[34] This is not limited to Google. Many of the tools we enjoy and rely on today do not partake in mass collection of data because it is technically necessary to do so, but because it is immensely profitable. Over the years, this has developed into a gross misdirection, wherein individuals, believing that collection of their data is an unavoidable part of the technology they use, are given a false choice between privacy and technology: "companies began to explain these violations as the necessary

[27] Patricia A. Norberg, Daniel R. Horne and David A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs* 41, no.1 (2007); Bettina Berendt, Oliver Gunther & Sarah Spiekermann, "Privacy in e-commerce: Stated preferences vs. actual behavior," *Communications of the ACM* 48, no. 4 (2005).
[28] Martin Abrams, John Abrams, Peter Cullen & Lynn Goldstein, "Artificial Intelligence, Ethics and Enhanced Data Stewardship," *The Information Accountability Foundation*, (September 2017): 6.
[29] Sylvia E. Peacock, "How web tracking changes user agency in the age of Big Data; the used user," *Big data and Society*, vol.1, no.2 (2014).
[30] Brigid Richmond, "A Day in the Life of Data," *Consumer Policy Research Centre* (2019): 3.
[31] UK Information Commissioner's Office, "Big data, artificial intelligence, machine learning and data protection," *Discussion Paper*, (2017): 24.
[32] Meyers West, "Data Capitalism," 37.
[33] Shoshanna Zuboff, *The Age of Surveillance Capitalism* (London: Profile Books, 2019), 15.
[34] James A. Buczynski, "The Googlization of Everything: And Why We Should Worry," *Library Journal* 136, no. 7 (2011): 109.

quid pro quo for "free" internet services. Privacy, they said, was the price one must pay for the abundant rewards of information, connection and other digital goods, when, where and how you want them."[35]

And yet, blaming technology for the erosion of privacy is like blaming a skeleton for the movements performed by muscles. Technology itself is not the cause of privacy erosion, rather, it is the underlying ideology that benefits from individuals believing that privacy invasion is inevitable. Technology is not developed in a silo, it is an expression of other agendas - and today that is in the interest of power accumulation through information asymmetries. The focus on consent and transparency in the privacy legislative landscape may once have had best intentions to empower individuals, but this has mutated into a way to actually reduce consumers' ability to exercise control over their privacy. The fact that people do not even engage with, let alone understand the complex system of pervasive data collection, use and disclosure is *by design.*

There are many pieces to this puzzle, which in itself makes it a challenge for both consumers and policymakers. Information privacy norms have centred individuals with the intention of empowering them to be able to control their data. Unfortunately, this has contributed to a system in which consumers have no *real* power over the flows of their data. This has been exacerbated by some key players in the technology industry by pushing the 'trade-off' narrative by positioning mass data collection as a technological necessity that must be endured (and consented to). We *know* people still care about privacy, however the current privacy landscape in Australia has laid the foundation for a paradox in which people are expected to exercise control over their privacy, but are not given meaningful ways to do so. While individual autonomy will always be important in privacy, attention needs to be redirected toward the practices of companies and government organisations. Where the power lies, so should to the responsibility.

Bibliography

Abrams, Martin, John Abrams, Peter Cullen, and Lynn Goldstein. "Artificial intelligence, ethics, and enhanced data stewardship." *IEEE Security & Privacy* 17, no. 2 (2019): 17-30.

Australian Law Reform Commission. *Managing Discovery: Discovery of Documents in Federal Courts (ALRC Report 115).* Australian Law Reform Commission, 2011. https://www.alrc.gov.au/publication/managing-discovery-discovery-of-documents-in-federal-courts-alrc-report-115/12-professional-and-ethical-discovery-2/potentially-unethical-discovery-practices/

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. "Privacy in e-commerce: stated preferences vs. actual behavior." *Communications of the ACM* 48, no. 4 (2005): 101-106

Buczynski, James A. "The Googlization of Everything: And Why We Should Worry." *Library Journal* 136, no. 7 (2011): 109.

boyd, danah, and Alice E. Marwick. "Social privacy in networked publics: Teens' attitudes, practices, and strategies." In *A decade in internet time: Symposium on the dynamics of the internet and society* (2011).

[35] Zuboff, *The Age of Surveillance Capitalism*, 52.

Campolo, Alex, Madelyn Sanfilippo, Meredith Whittaker, and Kate Crawford. "AI now 2017 report." *AI Now Institute at New York University* (2017). https://ainowinstitute.org/AI_Now_2017_Report.pdf.

Cate, Fred H., Peter Cullen, and Viktor Mayer-Schönberger. "Data protection principles for the 21st century: revising the 1980 OECD guidelines." *Redmond, WA: Microsoft Corporation* (2014).

Culnane, Chris, Benjamin IP Rubinstein, and Vanessa Teague. "Health data in an open world." *arXiv preprint arXiv:1712.05627* (2017).

Department of Treasury and Finance, "Regulating in the digital age, Government Response and Implementation Roadmap for the Digital Platforms Inquiry," 12 December 2019, Australian Government. https://treasury.gov.au/publication/p2019-41708

International Conference of Data Protection & Privacy Commissioners. "International Resolution on Privacy as a Fundamental Human Right and Precondition for exercising other fundamental rights." *41st International Conference of Data Protection and Privacy Commissioners*, October 2019. https://edps.europa.eu/sites/edp/files/publication/resolution-on-privacy-as-a-fundamental-human-right-2019-final_en.pdf

Kemp, Katherine and Rob Nicholls. "The federal government's response to the ACCC's Digital Platforms Inquiry is a let down," *The Conversation*, 12 December, 2019. https://treasury.gov.au/publication/p2019-41708

McDonald, Aleecia M., and Lorrie Faith Cranor. "The cost of reading privacy policies." *Isjlp* 4 (2008).

Norberg, Patricia A., Daniel R. Horne, and David A. Horne. "The privacy paradox: Personal information disclosure intentions versus behaviors." *Journal of consumer affairs* 41, no. 1 (2007): 100-126.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services." *Information, Communication & Society* 23, no. 1 (2020): 128-147.

Office of the Australian Information Commissioner. "Chapter B: Key Concepts," in *Australian Privacy Principle Guidelines.* https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/

OAIC. "What is personal information", *Factsheet*, May 2017. Available at https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information

Office of the Privacy Commissioner of Canada, "Consent and Privacy," *Discussion paper,* May 2016. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

Office of the Victorian Information Commissioner (OVIC). "To consent and beyond." *Blogpost,* 7 January, 2020. https://ovic.vic.gov.au/blog/to-consent-and-beyond-are-no-go-zones-the-next-frontier-part-1/

Peacock, Sylvia E. "How web tracking changes user agency in the age of Big Data: The used user." *Big Data & Society* 1, no. 2 (2014): 2053951714564228.

Pearson, Siani, and Marco Casassa-Mont. "Sticky policies: An approach for managing privacy across multiple parties." *Computer* 44, no. 9 (2011): 60-68.

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S. and Dabbish, L., 2013. Anonymity, privacy, and security online. *Pew Research Center* (2013). http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Richmond, Birgid. "A Day in the Life of Data: Removing the opacity surrounding data collection, sharing and use environment in Australia." Consumer Policy Research Centre, Research Report, 2019. https://cprc.org.au/wp-content/uploads/CPRC-Research-Report_A-Day-in-the-Life-of-Data_final-full-report.pdf

Rose, J., C. Barton, R. Souza, and J. Platt. "The trust advantage: How to win with big data, November." *Boston: Consulting Group* (2013). www.bcgperspectives.com/content/articles/information_technology_strategy_consumer_products_trust_advantage_win_big_data

Rule, James and Greenleaf, Graham, eds. *Global Privacy Protection: The First Generation.* Cheltenham: Edward Elgar, 2008.

Solove, Daniel, J. "Conceptualizing Privacy." *California Law Review* 90, no. 4, 2002.

UK Information Commissioner's Office (ICO), "Big data, artificial intelligence, machine learning and data protection," Discussion Paper, 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

West, Sarah Myers. "Data capitalism: Redefining the logics of surveillance and privacy." *Business & society* 58, no. 1 (2019): 20-41.

Zuboff, Shoshana. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books, 2019.