Data Ownership and Privacy: Investigating a Shared Psychological Basis

Breanna Amoyaw (amoyawb1@myumanitoba)
Department of Psychology, University of Manitoba

Katie Szilagyi (katie.szilagyi@umanitoba.ca)
Faculty of Law, University of Manitoba

Shaylene E. Nancekivell (shaylene.nancekivell@umanitoba.ca)
Department of Psychology, University of Manitoba

Abstract

People often share their personal data online despite reporting that they should not. They also show surprise and distress when data is used in ways they authorize despite giving consent. But, what underlies this inconsistency in people's thinking? In the present study, we investigated the proposal that thinking about control over information, or informational autonomy, likely underlies variability in thinking about privacy and data ownership. Namely, we propose that threats to one's autonomy might account for the aforementioned changes in people's concern for their data. To test this account, we used a surveystyle design to measure how a hypothetical threat to the self, and thereby control, influenced adults' ($N = 51$) judgments about the ownership and privacy of their personal data. The threat was police lawfully obtaining their data with a warrant. We found that privacy and ownership judgments significantly increased over time. We also found that the variability in participants' ownership and privacy judgments was related. Together, our findings suggest that privacy and ownership likely have a shared psychological basis, and this shared psychology can likely explain the variability in people's judgments about personal data across time.

Keywords: privacy; ownership; personal data; information; threat; control

Introduction

For many people, online applications (apps) are highly integrated in everyday life. The average person with a smartphone uses 10 different apps per day (G, 2024) that serve a variety of purposes, such as online shopping, social media, online banking, navigation, and listening to music. People share both highly identifying personal information within apps, such as their name, phone number, or email address as well as less identifying data, such as their location, app usage, search history, device information, Wi-Fi connections, and more (Polykalas & Prezerakos, 2019). Notably, how people think about their personal data in online contexts often appears inconsistent and difficult to predict. People get upset about their data being used by apps in ways to which they initially agreed; people sue over third parties using the very data they shared with them and gave-up control of; or intention-behavior gaps where people claim it is important to keep their data safe, but then fail to take steps to protect it *in situ* (e.g., Afriat, 2021; Hinds et al., 2020; Kokolakis, 2017; Norberg, 2007; Tuttle, 2018).

What causes these seemingly inconsistent judgments? One possibility is that these judgments do not represent inconsistency at all. For example, people may simply be confused by the complexity of online environments leading them to seem inconsistent from interface to interface (e.g., complexity accounts; Tredinnick, 2009); people might find protecting their data too difficult and so sometimes behaviorally do not take the steps they need to protect their data (e.g., intention-behavior paradox; Kokolakis, 2017); or people are unsure as to what they are consenting to when they use apps, meaning their behavior is not inconsistent at all but stems from confusion experienced at different time points (e.g., consent confusion; Benoliel & Becher, 2019; Solove, 2024). Under these common accounts, people's beliefs are staying constant, but confusion, effort, and/or complexity are making it difficult for them to behave consistently over time. However, another more psychologically interesting possibility is that people's beliefs about their data are indeed changing from time point to time point. *But, if this is the case, then what psychological processes are influencing people's changing beliefs?*

As with any complex phenomenon, there is likely more than one factor contributing to its complexity. Here, we explore two overlapping psychological variables that likely influence people's judgments from time point to time point: beliefs about privacy importance and feelings of ownership. Namely, we test the specific proposal that: i) people's beliefs about privacy and ownership overlap or have a shared psychological basis, and ii) they can change across time and within the same individual.

Although previously overlooked in the literature, the psychology of privacy and ownership likely have a shared or overlapping basis. In the context of data, they are both related to one's ability to control or make autonomous decisions

In D. Barner, N.R. Bramley, A. Ruggeri and C.M. Walker (Eds.), *Proceedings of the 47th Annual Conference of the Cognitive Science Society*

about their information. For example, the Charter of Fundamental Rights of the European Union highlights the protection of personal data. Article 8 states that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned…" (Charter of Fundamental Rights of the European Union, 2012). Here, we propose that thinking about control over information, or informational autonomy, likely underlies thinking about privacy and data ownership. Indeed, one notable theory of privacy by Fried (1984) frames it as "not just an absence of information abroad about ourselves; it is a feeling of security in control over that information." Most relevant for the current proposal, a control-based account of privacy places informational autonomy at the heart of privacy, as it highlights how privacy includes one's ability to control their personal information across contexts. Furthermore, development of the individual in democratic society is enabled through privacy's guarantees of protection for the core self, permitting basic functions like cultivation of personal autonomy, emotional release, self-evaluation, and ensuring limited and protected communications are possible (Westin, 1967).

Indeed, qualitative work asking people to define privacy using drawings has found that experts and non-experts both spontaneously include elements related to controlling information like passwords and locks, indicating that it is a central part of their representations (Oates et al., 2018). Similarly, autonomy or control is thought to be central to ownership psychology (e.g., Nancekivell et al., 2019). For example, touching or even imagining touching a target elicits feelings of ownership as it produces feelings of control or autonomy (Peck et al., 2013; Peck & Shu, 2009). The legal literature further supports this idea; many legal cases related to data privacy are focused on contesting ownership of the information (e.g., *McInerney v. MacDonald,* 1992; *R v. Bykovets,* 2024). Further, we know from diverse works across human-computer interaction and psychology that children and adults will express that they own their personal information or data (e.g., Agesilaou & Kyza, 2022; Cichy, 2014; Nancekivell & Fahey, 2022) and that this is important to them.

Before we continue, it is worth noting that in the present study we are specifically studying people's beliefs about psychological ownership or feelings of ownership. Prior work has established that people can feel ownership, known as psychological ownership, of entities they may or may not legally own (Friedman et al., 2018; Peck & Luangrath, 2018; Pierce et al., 2003). Psychological ownership is defined as the state in which individuals feel as though an entity is "theirs" (i.e., it belongs to them; Pierce et al., 2003). Psychological ownership can apply to a wide range of targets, from tables at a restaurant to ideas (Hingston et al., 2024; Kirk et al., 2018; Shaw et al., 2012). We focus on psychological ownership as it is more likely to vary across time points as compared against legal ownership (owned vs. not owned), which is often thought to be more categorical in nature and thus is less likely to vary across time.

In the present study, we will test our proposal by examining how a threat to one's autonomy over their data or "threat to the self" influences privacy and ownership judgments. The idea that a threat to the self may increase psychological ownership of personal data comes from territoriality accounts of ownership, which suggest that when control or autonomy is threatened, ownership signals increase (e.g., Kirk et al., 2018). In this study, we measure privacy and ownership beliefs before and after the threat. If ownership and privacy are intertwined via shared locus of autonomy, then we would expect both feelings of privacy and ownership to increase after such a threat.

The Present Study

The present study included one within-subjects experiment which measured people's beliefs about minimally identifying data before and after a threat to the self. Minimally identifying data (i.e., device type, previously viewed product videos, and Wi-Fi network name) were chosen as we needed a variable that would not show a ceiling effect on our target measures. That is, feelings of ownership of highly identifying data such as a person's name, home address, or phone number, would likely already elicit strong feelings of ownership and privacy even before a threat is introduced.

In the study, participants were told that the police are investigating a crime and have a warrant which allows them to search an app they have used for information about all its users. We used the police as the threat to the self as they are an authority figure that would reasonably be able to access personal data from an app in a legal manner (e.g., Koops, 2013). We also selected the police as the threat since they are often involved in investigations related to digital crime (Bryant & Kennedy, 2016). Further, the police would be viewed as having complete control over the data after obtaining it, which should trigger participants to feel their control or autonomy is threatened.

Before and after the introduction of the threat, participants were asked three test questions. First, they were asked how much they feel they own their data. This question was modelled after prior studies on psychological ownership, emphasizing how much people feel like they own something (e.g., Cleroux et al., 2022; DeScioli & Karpoff, 2015; Peck & Shu, 2009). Second, participants were asked how important they feel it is to keep their personal data private, as personal importance of privacy is often one of the ways that privacy is discussed and measured in the literature (e.g., Kokolakis, 2017). Lastly, as a control measure, participants were asked how helpful they feel their personal data is to them (i.e., to capture any general tendencies to go "up a scale" when asked a question twice). We predicted that target ratings of ownership and the importance of privacy would increase from before the threat (i.e., time 1) to after the threat (i.e., time 2), but perceived helpfulness of personal data should not change in the presence of a threat.

Method

Participants

The sample consisted of 51 adults (M_{age} = 19.8 years old) from a university-level introductory psychology course. The sample identified as 74.5% women and 25.5% men. The racial/ethnic identities of participants in the sample were: 35.3% White, 33.3% Asian, 15.7% Black, 7.8% multiracial, 2.0% First Nations/Inuit/Metis, 2.0% Latin American, 2.0% Arab, and 2.0% other. We are still collecting data. Participants were recruited from an undergraduate participant pool and were awarded with research credit toward their introduction to psychology course. Fourteen have been excluded so far for not passing the comprehension questions, attention checks, and/or commitment check. The experimental protocol for this study was approved by the research ethics board at the host institution.

Materials and Procedure

Participants independently completed the study in-person in a computer lab and the study survey was hosted online on Qualtrics. The study began by informing participants that they would be asked to make some judgments and to read the following text carefully. After this message, participants were presented with an introduction that stated: "Imagine that you downloaded a new e-commerce app from the app store. The app can be used to purchase many different kinds of products (e.g., clothes, electronics, books, etc.). This app stores information about its users, including you. When you downloaded the app, you agreed to the terms and conditions, including giving the app permission to store information about you and your app usage." To check if participants understood the prompt, it was immediately followed by a comprehension question (see Table 1). The study also included two attention checks and a commitment check (see Table 1).

Table 1: The items and inclusion/exclusion criteria for the data quality checks.

Type of data quality check	Item	Inclusion/exclusion criteria
Comprehension check	What is the app used for?	Must mention purchasing/buying products, online shopping, and/or e-commerce
Comprehension check	Are the police searching the app for information you shared?	Must answer Yes
Attention check	To answer this question, please select six.	Must answer 6
Attention check	Who was mentioned during the study?	Must answer Police
Commitment check	It is important to us that participants paid close attention to the questions. Did you provide thoughtful answers to all the questions in this survey?	Must answer Yes

After the introduction, participants were presented with three trials to measure their feelings about different types of minimally identifying data. The types of data included device type, previously viewed product videos, and Wi-Fi network name. Each trial started by stating that the app stores the specific type of information as data on its servers. Then, participants judged their feelings of ownership, privacy, and helpfulness of the specific type of data (see Table 2 for questions). Responses were recorded using a 10-point Likert scale (see Table 2 for endpoints). The type of judgment (i.e., ownership, privacy, and helpfulness) was counterbalanced using a Qualtrics randomizer as was the order of the different types of data.

After completing the first half of the study, participants were presented with a prompt which served as a threat to the self. The prompt stated: "The police are investigating a crime. They suspect everyone that used the app was involved. They have a warrant which allows them to search the app to retrieve information about its users. They are searching the app for information you shared." The prompt was followed by a second comprehension question (see Table 1). Participants then made their judgments a second time (see Table 2 for questions). Participants were reminded of their response given at time 1 with the statement "Previously you gave this item a score of [insert previous response]." The same counterbalancing was used at time 2 as time 1. After completing the main study questionnaire, participants justified as to why or why not their feelings about the information changed after the police searched the app.

Table 2: The outcome variables, question wording, and endpoints for the survey questions. Device type/previously viewed product videos/Wi-Fi network name go where [insert data type] is written.

Outcome variable	Item	Endpoints (1 to 10 Likert scale)
Ownership	How much do you feel data about your [insert data type] belongs to you?	1 (Not at all) 10 (A lot)
Privacy	How important do you feel it is to keep data about your [insert data type] private?	1 (Not at all) 10 (Very)
Helpfulness	How much do you feel data about your [insert data type] helps you?	1 (Not at all) 10 (A lot)

Results

The first hypothesis we investigated was how participants' judgments changed before and after the threat manipulation. We predicted that ownership and privacy judgements would increase due to their overlapping roots in autonomy. To test this hypothesis, we specifically ran a repeated measure ANOVA with main effects of judgment and time, and a judgement by time interaction.

Participants' responses differed by judgment, $F(2, 100) = 7.56$, $p < .001$ and time $F(1, 50) = 12.98$, $p < .001$. Most crucially, there was an interaction by judgement and time, $F(2, 100) = 6.37$, $p = .002$. Follow-up paired samples t-tests revealed that participants' privacy judgments increased after

the threat, $t(50) = -4.24$, $p < .001$ by an average of .62 increase (SD = 1.05). Ownership judgments significantly differed from time 1 to time 2, $t(50) = -2.06$, $p = .044$ and there was an average increase of .28 (SD = .97). Finally, help judgments, our control, did not differ, $t(50) = .44$, $p = .66$. Here, judgments on average decreased by .07 (SD = .85).

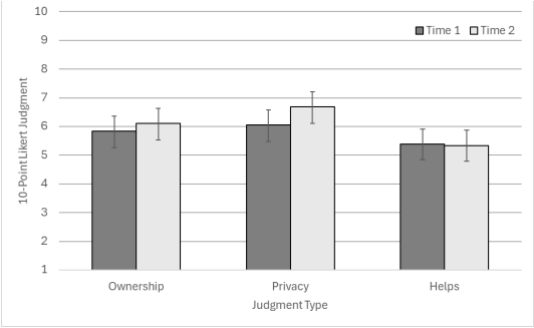

Figure 1: Bar graph showing the average ratings at both time 1 and time 2 divided by judgment type. Errors bars depict standard error.

In examining our data, we noticed a sizable amount of variation in participants' responsiveness to the threat; namely ownership (and privacy) judgements had a standard deviation of around 2.00 on a 10-point scale, which is rather large. At the end of our task, participants were asked to explain their thinking. In these explanations, we found variability in participants' responsiveness to the threat. Namely, some participants discussed feeling vulnerable and uncomfortable with the police using their data due to a lack of control over it as predicted. But, we also found that others reported trusting the police and appeared to not feel any sort of threat or discomfort. For example, one participant, compatible with our predictions, said "...my data was also being looked at and deciphered by someone of higher power which made me feel vulnerable.…" while another said "...if I had been using the app responsibly, I would have no fear in police checking my data." Table 3 provides some examples of each explanation type.

Table 3: Sample explanations from the open-ended question at the end of the task.

Perceived threat	No perceived threat
"...my data was also being looked at and deciphered by someone of higher power which made me feel vulnerable.…"	"...if I had been using the app responsibly I would have no fear in police checking my data."
"…my feelings especially related to the privacy of my information changed as authorities accessing the data leaves me in a vulnerable spot like it was in the situation provided."	"…as I haven't committed a crime as to my knowledge, I don't really care that the police obtained access to my information."
"…I feel that if they need certain information they should ask the person for permission as well, instead of just being allowed the information due to their authority."	"…I saw the valuable use of this stored data in aiding the police in successfully finding the criminal."
"…Once I realized they are actively accessing my data, I felt more protective of my data. I did not want my data shared anymore.	"…nothing I do on an app is of any interest to the police."

To this end, we next conducted some unplanned exploratory analyses to understand how variation in ownership judgments was potentially related to variation in privacy judgments. Based on the proposed theory that privacy and ownership have shared psychology, we hypothesized that we should be able to detect a relationship between variation in ownership and privacy judgments. To test this relation, we first created differences scores for each judgment type representing participants responsiveness to the threat. Specifically, time 1 judgments were subtracted from time 2 judgments. We found that privacy and ownership differences scores had a moderate positive correlation, $r = .40$, $p = .004$. Next, we tested for correlations among help judgments and ownership/privacy to understand if low-level response tendencies might explain the target relation. Here we found that help difference scores were not correlated with ownership difference scores, $r = -.157$, $p = .27$, or privacy difference scores, $r = -.26$, $p = .062$. Thus, low-level response tendencies like tendencies to "up a scale" likely do not explain the target correlation. Altogether, we found that variation in ownership judgments was likely related to variation in privacy judgments.

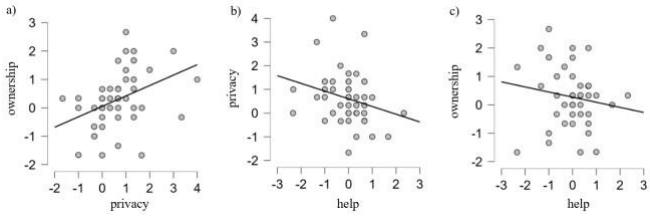

Figure 2: Correlations of (a) privacy and ownership difference scores, (b) privacy and help difference scores, and (c) ownership and help difference scores.

Discussion

In sum, we found that ratings of the importance of privacy and ownership increased at a group level in response to our threat. Judgments of helpfulness did not differ at all. Exploratory correlational analyses revealed that variation in privacy judgments was indeed related to variation in ownership judgments, as privacy difference scores increased with ownership difference scores. Together, these findings suggest that feelings of ownership and privacy likely have some overlapping basis. Next, we discuss our findings in further detail. However, before doing so, it is worth noting that all findings are preliminary as data collection is still ongoing.

We found that feelings about privacy changed in response to the threat to the self. Namely, when control over personal information was threatened by the police, the importance of privacy increased. We argue that this was likely to regain autonomy over personal information. Participants' openended responses support this idea. As shown in Table 3, participants mentioned feeling a lack of control or vulnerability.

We also found that feelings about ownership changed in response to the threat to the self. This was compatible with our predictions, as autonomy and control have been argued to be central to ownership psychology (e.g., Nancekivell et al., 2019). For instance, touching a target and exerting control over it is enough to elicit feelings of ownership (Peck et al., 2013; Peck & Shu, 2009). Here we find, compatible with prior work, that people's feelings of ownership over their data increased in response to our threat manipulation. This finding has a few implications. For one, it demonstrates that similar to data privacy judgments, psychological ownership judgments are not stagnant and can change over time. Additionally, it highlights how threats to the self may be a main mechanism through which these judgments are triggered. Importantly, these findings contribute to the evolving literature on how ownership thinking is used to reason about personal data (e.g., Agesilaou & Kyza, 2022; Cichy, 2014; Nancekivell & Fahey, 2022).

These results also provide support for our theory of a shared or overlapping psychological basis of privacy and ownership. They are bolstered by our exploratory analysis where we also found a positive correlation between the difference scores of privacy and ownership judgements. This positive correlation further suggests a relation between privacy and ownership judgments, as it demonstrates that these judgements move together in response to a threat to the self.

Notably, this proposal is somewhat controversial as some have argued that privacy is not solely about control or access, but rather privacy needs to consider "who personal information is about, how it is transmitted, and past and future actions by both the subject and the users of the information" (i.e., contextual integrity framework; Barth et al., 2006; Nissenbaum, 2010). But, our findings further highlight how feelings of control are not binary (i.e., having control or not having control). Indeed, we find that feelings of control appear to vary from time point to time point within individuals and influence privacy and ownership thinking. Integrating our perspective with Nissenbaum, it could be that the contextual factors she focuses on may be influencing privacy (and ownership) by influencing beliefs about autonomy and control.

It is also worth noting that ownership judgments increased an average of .28 while privacy judgments, on average, increased double this amount. One possible explanation is that participants might have had difficulty in dissociating legal (actual) ownership and feelings of ownership. If participants in our study conflated legal ownership with psychological ownership when answering our scale, it may have led some participants to be less responsive to the manipulation as legal ownership likely does not vary to this degree (i.e., one typically lawfully owns something or not). We hope to explore this issue in follow-up experiments.

Relatedly, we found that not all participants felt threatened by the manipulation. Indeed, standard deviations at time 2 were very large for both privacy and ownership judgments. Coding of the explanations suggests that participants fall into two distinct categories, as seen in Table 3. Future experiments should directly test this proposal by utilizing a different authority figure for the threat manipulation, such as a professor or school administrator that students might universally respond to. Future work should also incorporate measures of individual differences to help capture differences in responses to the threat. Doing so would allow researchers to determine individuals' comfort with and trust in authority figures. Future work may also dive deeper into the individual differences in threat perception and what caused them. This difference is worth exploring, as one possible reason as to why some participants may have felt more threatened than others could be that they felt they personally committed the crime in question. The degree to which participants deem the shared data as incriminating could also be an important factor to consider in future research.

Limitations of the present study should also be considered. For one, participants in the present study had a mean age of 19.8 years old. This may limit the generalizability of the findings to other populations, such as older adults. Future work should address this limitation by replicating the study with other samples that include different age demographics. Overall, this is a single experiment paper with one threat as the manipulation, so it is important for future research to replicate these findings with other threats and with other populations as the sample.

Altogether, this study is the first to provide some evidence for a shared psychological basis between data privacy and data ownership. Specifically, we found some initial support for our hypothesis that control and autonomy are likely central to both judgments. We argue that attending to contextual differences in how and when people experience threats to the self, as it relates to their autonomy and control, can likely help us better understand the variability that exists in people's judgments about their personal data over time.

Acknowledgments

This research was supported by funding from the Natural Science and Engineering Research Council of Canada (NSERC) Discovery Grant awarded to SN. We would also like to acknowledge the Centre for Professional and Applied Ethics at the University of Manitoba for their support through a fellowship awarded to SN.

References

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2020). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society, 37*(2), 115–127. https://doi.org/10.1080/01972243.2020.1870596

Agesilaou, A., & Kyza, E. A. (2022). Whose data are they? Elementary school students' conceptualization of data ownership and privacy of personal digital data. *International*

Journal of Child-Computer Interaction, 33, 100462. https://doi.org/10.1016/j.ijcci.2022.100462 Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In *2006 IEEE Symposium on Security and Privacy.* https://doi.org/10.1109/SP.2006.32

Benoliel, U., & Becher, S. I. (2019). The duty to read the unreadable. *Boston College Law Review, 60*(8), 2255–2296.

Bryant, R., & Kennedy, I. (2014). Investigating digital crime. In R. Bryant & S. Bryant (Eds.), *Policing digital crime*. Ashgate Publishing Limited. https://doi.org/10.4324/9781315601083

Cichy, P., Salge, T. O., & Kohli, R. (2014). Extending the privacy calculus: the role of psychological ownership. *Thirty Fifth International Conference on Information Systems*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=092daf3f68f0ad4dc735dc7f958f3bd5e4946d34

Cleroux, A., Peck, J., & Friedman, O. (2022). Young children infer psychological ownership from stewardship. *Developmental Psychology, 58*(4), 671–679. https://doi.org/10.1037/dev0001325

DeScioli, P., & Karpoff, R. (2015). People's judgments about classic property law cases. *Human Nature, 26*(2), 184–209. https://doi.org/10.1007/s12110-015-9230-y

European Union. (2012). Charter of Fundamental Rights of the European Union, Article 8. *Official Journal of the European Union* C 326/391

Fried, C. (1984). Privacy [a moral analysis]. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy*: *An anthology*. Cambridge University Press. https://doi.org/10.1017/CBO9780511625138.008

Friedman, O., Pesowski, M. L., & Goulding, B. W. (2018). Legal ownership is psychological: Evidence from young children. In J. Peck, & S. B. Shu (Eds.), *Psychological ownership and consumer behavior*. Springer International Publishing AG. https://doi.org/10.1007/978-3-319-77158-8_2

G, N. (2024, January 3). *55+ jaw dropping app usage statistics in 2024 [infographic]*. Techjury. https://techjury.net/blog/app-usage-statistics/

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies, 143,* 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Hingston, S. T., Tian, L., & Deska, J. C. (2024). Cues of trait dominance elicit inferences of psychological ownership. *British Journal of Social Psychology, 64*(1), e12819. https://doi.org/10.1111/bjso.12819

Kirk, C. P., Peck, J., & Swain, S. D. (2018). Property lines in the mind: Consumers' psychological ownership and their territorial responses. *The Journal of Consumer Research, 45*(1), 148–168. https://doi.org/10.1093/jcr/ucx111

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Koops, B.-J. (2013). Police investigations in Internet open sources: Procedural-law issues. *The Computer Law and Security Report, 29*(6), 654–665. https://doi.org/10.1016/j.clsr.2013.09.004

McInerney v. MacDonald, [1992] 2 SCR 138.

Nancekivell, S. E. & Fahey, J. (2022). Who owns your information? Young children's judgments of who owns the general and personal information users share with apps. In J. Culberston, A. Perfors, H. Rabagliati, & V. Ramenzoni (Eds.), *Proceedings of the 44th Annual Meeting of the Cognitive Science Society.* https://escholarship.org/uc/item/5550136d

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. https://doi.org/10.1016/j.tics.2018.11.008

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford Law Books. https://doi.org/10.1515/9780804772891

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). Privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs, 41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Oates, M., Ahmadullah, Y., Marsh, A., Swoopes, C., Zhang, S., Balebako, R., & Cranor, L. F. (2018). Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies, 2018*(4), 5–32. https://doi.org/10.1515/popets-2018-0029

Peck, J., & Shu, S. B. (2009). The effect of mere touch on perceived ownership. *Journal of Consumer Research, 36*(3), 434–447. https://doi.org/10.1086/598614

Peck, J., Barger, V. A., & Webb, A. (2013). In search of a surrogate for touch: The effect of haptic imagery on perceived ownership. *Journal of Consumer Psychology, 23*(2), 189–196. https://doi.org/10.1016/j.jcps.2012.09.001

Peck, J., & Luangrath, A. W. (2018). Looking ahead: Future research in psychological ownership. In J. Peck, & S. B. Shu (Eds.), *Psychological ownership and consumer behavior*. Springer International Publishing. https://doi.org/10.1007/978-3-319-77158-8

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology, 7*(1), 84–107. https://doi.org/10.1037/1089-2680.7.1.84

Polykalas, S. E., & Prezerakos, G. N. (2019). When the mobile app is free, the product is your personal data. *Digital Policy, Regulation and Governance, 21*(2), 89–101. https://doi.org/10.1108/DPRG-11-2018-0068 *R v. Bykovets,* 2024 SCC 6.

Shaw, A., Li, V., & Olson, K. R. (2012). Children apply principles of physical ownership to ideas. *Cognitive Science, 36*(8), 1383–1403.

Solove, D. J. (2024). Murky consent: an approach to the fictions of consent in privacy law. *Boston University Law Review, 104*(2), 593-640.

Tredinnick, L. (2009). Complexity theory and the web. *Journal of Documentation, 65*(5), (797-816). https://doi.org/10.1108/00220410910983119

Tuttle, H. (2018). Facebook scandal raises data privacy concerns. *Risk Management, 65*(5), 6-9. https://link.gale.com/apps/doc/A538250056/AONE?u=anon~2e8f83b2&sid=googleScholar&xid=26024cdb

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.