OWNERSHIP OF PERSONAL INFORMATION?

DONRICH THALDAR[†]
Professor of Law, University of KwaZulu-Natal

This article explores whether personal information can be owned and, if so, by whom. It begins with an overview of fluctuating judicial attitudes toward personal information ownership, highlighting the need for a thorough analysis of how the foundational tenets of ownership apply to personal information, particularly in digital form. The analysis clarifies that ownership is a concept rooted in property law, necessitating that questions of personal information ownership be answered within the ambit of property law, rather than informational privacy law. Building on this theoretical base, it becomes clear that while personal information in general does not meet the criteria for ownership, a specific digital instance of such information — that is, a computer file containing personal information — indeed meets the criteria and is therefore susceptible of ownership. When a new instance of information is generated, property law dictates that the first person to exercise control over it with the intent of ownership thereby becomes its owner. However, the data subject's informational privacy rights impose limitations on the owner's property rights. This interplay between informational privacy law and property law lays a crucial foundation for the legal governance of personal information in the digital age.

Informational privacy – ownership – personal information – property – res nullius

I INTRODUCTION

'Personal information' (or 'personal data') is generally understood as information (or data) that pertains to an identified or identifiable natural person. This definition is underscored by several international frameworks and conventions, including the Organisation for Economic Co-operation and Development's Guidelines,[1] the Council of Europe's Convention 108[2] and the African Union Convention on Cyber Security Personal Data Protection.[3] In an intriguing deviation, South Africa's Protection of Personal Information Act 4 of 2013 ('POPIA') broadens this definition to encompass juristic persons in appropriate contexts.[4]

[†] BLC LLB MPPS (Pretoria) PhD (Cape Town) PGDip (Oxon). *https://orcid.org/0000-0002-7346-3490*. The majority of this work was prepared while I was a Visiting Scholar at the Petrie-Flom Center, Harvard Law School, in 2022.

[1] Organisation for Economic Co-operation and Development ('OECD') *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information*, 23 September 1980.

[2] Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Information*, 28 January 1981, ETS No 108.

[3] African Union *African Union Convention on Cyber Security Personal Data Protection*, 27 June 2014 ('the Malabo Convention').

[4] POPIA, s 1.

https://doi.org/10.47348/SALJ/v142/i1a10

POPIA articulates a comprehensive, though not exhaustive, array of examples of what constitutes personal information.[5] These examples include, but are not limited to, details concerning an individual's race, gender, sexual orientation, physical or mental health, religious beliefs, and language; their educational, medical, financial, criminal, or employment history; various identifying particulars such as email addresses, physical addresses, and biometric information; personal opinions, preferences, and correspondence; as well as the views or opinions expressed about the individual. Notably, the inclusion of a person's name is also considered personal information if it is presented in conjunction with other personal details or if its disclosure alone would reveal further information about the individual.[6]

In accordance with its title and as articulated in its long title, the principal objective of POPIA is to promote the protection of personal information. Nevertheless, POPIA concurrently engages in a nuanced equilibrium: it recognises that the advancement of economic and social interests necessitates the elimination of unwarranted obstacles that impedes the free flow of information. Further, POPIA's preamble elucidates that this free flow of information ought to be balanced with the constitutional right to privacy. This right encompasses the protection of personal information from unlawful processing.

In the contemporary landscape of lightning-speed information highways and sophisticated analysis of information through artificial intelligence algorithms, there has been an exponential increase in the volume of information. Information — including *personal information* — is fuelling the digital economy, and this fuel often carries a monetary value.[7]

In practical terms, personal information has evolved into a commodity. While the commodification of personal information is frequently linked with social media entities, its scope extends far beyond them, permeating the entirety of the digital economy. An illustrative example is that of a firm engaged in direct-to-consumer genetic testing, which, presumably with the consent of its consumers, collects their genetic information and subsequently monetises it through sales or licensing agreements with biopharmaceutical companies for use in precision medicine research.[8] This situation foregrounds a critical legal question: is it possible to assert ownership over personal information and, if so, who holds such ownership?

[5] Ibid.

[6] Ibid.

[7] James Nurton 'Data: The fuel transforming the global economy' 2022 *WIPO* available at *https://www.wipo.int/wipo_magazine_digital/en/2022/article_0002.html*, accessed on 27 March 2024.

[8] See for example Amy Gooden & Donrich Thaldar 'Direct-to-consumer genetic testing in South Africa: Stumbling over the first legal hurdle?' (2022) 25 *PER/PELJ* 1.

https://doi.org/10.47348/SALJ/v142/i1a10

The current South African legal academic literature does not provide a definitive answer. Njotini suggests that because of the proliferation of information in our modern society, and the interests that governments, businesses and individuals have in such information, the law should develop to include information as an object of property rights.[9] Erlank dedicates an article to investigating the concept of 'virtual property' and makes a convincing case that 'digital objects' (such as websites, email addresses, bank accounts, e-books, smartphone apps and digital music) are indeed capable of being owned in our extant property law.[10] However, whether it is possible for personal information to qualify as a 'digital object' was not part of Erlank's investigation. I intend to explore this fully in the analysis that follows.

In addressing the question whether personal information can be owned and, if so, by whom, I draw on the work that I have done with colleagues on the ownership of human genomic information — a specific type of personal information[11] — and the practical consequences of owning such information.[12] I build on these insights to establish a framework for understanding the legal nature of personal information in general.

A clarification on terminology is pertinent: in various jurisdictions, the terms employed to describe key concepts in the context of protection of personal information laws vary. For example, in the European Union, India, Kenya and Nigeria, the preferred terms are 'data' and 'personal data'. This is evident in legislative texts such as the General Data Protection Regulation ('GDPR'),[13] the Kenyan Data Protection Act,[14] the Nigeria Data Protection Act,[15] and India's Digital Personal Data Protection Act.[16] Conversely, jurisdictions such as Australia, California, Canada and New Zealand employ the terms 'information' and 'personal information'.[17] The designation of the person to whom this personal data or personal

[9] Mzukisi Njotini 'Examining the "objects of property rights": Lessons from the Roman, Germanic and Dutch legal history' (2017) 50 *De Jure* 136.

[10] Wian Erlank 'Introduction to virtual property: Lex virtualis ipsa loquitur' (2015) 18 *PER/PELJ* 1.

[11] Donrich Thaldar, Beverley Townsend, Dusty-Lee Donnelly et al 'The multidimensional legal nature of personal genomic sequence data: A South African perspective' (2022) 13 *Frontiers in Genetics* 1.

[12] Donrich Thaldar 'The wisdom of claiming ownership of human genomic data: A cautionary tale for research institutions' (2024) *Developing World Bioethics* 1.

[13] General Data Protection Regulation 2016/679 (EU).

[14] Data Protection Act 24 of 2019 (Kenya).

[15] Nigeria Data Protection Act, 2023.

[16] Digital Personal Data Protection Act, 2023 (India).

[17] See the Privacy Act 1988 (Cth) (Australia); the California Privacy Rights Act (2020) (US); the Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (Canada); the Privacy Act, 2020 (New Zealand).

https://doi.org/10.47348/SALJ/v142/i1a10

information relates also varies. In the European Union, Kenya and Nigeria, the term 'data subject' is used, in alignment with Convention 108[18] and the Malabo Convention.[19] India, by contrast, uses 'data principal'. Jurisdictions such as Australia, Canada and New Zealand prefer the term 'individual', reflecting the language of the OECD Convention.[20] California's legislation refers to 'consumer'. South Africa presents a unique case, combining these terminologies. POPIA uses 'information', 'personal information', and, somewhat anomalously, 'data subject'. In this article, the terms as outlined in POPIA will be consistently used for coherence and clarity.

First, the scene is set with an overview in part II of three recent cases relevant to the topic of personal information ownership. The analysis is then presented in two parts. In part III, two domains of the law are differentiated, namely property law and informational privacy law. I suggest that the question of ownership falls in the domain of property law. In part IV, the rules of property law are applied to personal information to ascertain whether it can be owned and, if so, by whom. The analysis is positioned in our digital age, where information is typically digitised, and where human interaction with digital objects, such as digital money and word-processor documents ('soft copies'), has become the norm.

II A CONSPECTUS OF RECENT CASE LAW

The first case that is examined is *Black Sash Trust v Minister of Social Development* ('*Black Sash Trust*'),[21] which reflects common misconceptions in the academic discussions on information ownership. The second case is *Discovery Ltd v Liberty Group Ltd* ('*Discovery*').[22] While falling short of a clear embrace of personal information ownership, this judgment signals an important move in that direction. By contrast, the judgment in the third case, *Mazetti Management Services (Pty) Ltd v Amabhungane Centre for Investigative Journalism NPC* ('*Mazetti Management Services*'),[23] diverges from this trend. These three cases collectively introduce key issues and demonstrate the fluctuating jurisprudential perspectives on personal information ownership, setting the stage for the subsequent analytical exposition.

(a) Black Sash Trust

The case of *Black Sash Trust* was brought on an urgent basis and related to the payment of social grants by the South African Social Security

[18] Convention 108 op cit note 2.
[19] Malabo Convention op cit note 3.
[20] OECD guidelines op cit note 1.
[21] 2017 (3) SA 335 (CC).
[22] 2020 (4) SA 160 (GJ).
[23] 2023 (6) SA 578 (GJ).

https://doi.org/10.47348/SALJ/v142/i1a10

Agency ('SASSA'), and SASSA's controversial outsourcing of social grant payment services to a private company, Cash Paymaster Services (Pty) Ltd ('CPS').[24] In the relief that the Black Sash Trust sought on behalf of social grant beneficiaries, it requested the Constitutional Court, inter alia, to declare that SASSA was the *owner* of the personal information of grant beneficiaries and that CPS, at the end of its contract with SASSA, had to provide such information to SASSA and remove such information from CPS's possession.[25] There was clear concern that CPS could misuse the personal information of grant beneficiaries, which included their contact details and banking information.[26]

The Information Regulator (the implementation agency established by POPIA) was cited as the seventh respondent by the Black Sash Trust. The inaugural executive members of the Information Regulator had taken office only a few months before the case was launched and, at that stage, had not yet appointed any administrative or operational staff.[27] Although this caused a delay, they eventually briefed legal representatives and belatedly filed written argument.[28] The Information Regulator took a different position to the Black Sash Trust regarding the ownership of personal information. While the Information Regulator did not challenge the idea that personal information can be owned, it argued that the personal information was not owned by SASSA, but by the thousands of grant beneficiaries qua data subjects.[29] Furthermore, the Information Regulator argued that, as a general principle, data subjects can never be divested from ownership of their personal information.[30] The reason proffered by the Information Regulator was that the protections afforded by POPIA to data subjects are compatible only with ownership vesting in data subjects.[31]

However, during the hearing of the matter, the Black Sash Trust abandoned the declaration that it sought in respect of the ownership of the personal information by SASSA.[32] Accordingly, the court did not need to deal with the issue of personal information ownership in its judgment.

[24] *Black Sash Trust* supra note 21 para 23.

[25] Ibid.

[26] Ibid paras 23(c) and 23(e). For further coverage on CPS's misuse of the personal information of grant holders see Gabriella Razzano 'Sassa grants: The small information win hiding in the grant crisis' *Daily Maverick* 24 April 2017, available at *https://www.dailymaverick.co.za/opinionista/2017-04-24-sassa-grants-the-small-information-win-hiding-in-the-grant-crisis/*, accessed on 28 March 2024.

[27] Written submissions filed by the seventh respondent (the Information Regulator) in *Black Sash Trust* supra note 21 para 25.

[28] Ibid.

[29] Ibid.

[30] Ibid

[31] Ibid.

[32] Ibid.

https://doi.org/10.47348/SALJ/v142/i1a10

The court merely noted in passing that the Black Sash Trust 'accepts that this order is misconceived and has abandoned it'.[33] Misconceived in what way? And why? These questions were left unanswered. In any event, the court did not provide any ratio decidendi on the topic of personal information ownership, and therefore the issue remained undecided.

The analysis below shows that the argument that the Black Sash Trust had presented was indeed correct, and that it was the Information Regulator's argument that was misconceived.

(b) Discovery

The *Discovery* case involved three applicants: Discovery Ltd, along with its subsidiaries, Discovery Life Ltd and Discovery Vitality (Pty) Ltd. Discovery Ltd holds the position of sole shareholder for both its subsidiaries.[34] Discovery Life Ltd operates as an insurance provider. Individuals participating in any medical scheme under the Discovery umbrella have the option to join the Vitality programme by paying a monthly fee, which is administered by Discovery Vitality (Pty) Ltd.[35] The programme is designed to incentivise healthier living by its members through a points-based system.[36] By achieving specific health-related milestones, members accumulate points, elevating their Vitality status from the initial 'Blue' level to 'Bronze', 'Silver', 'Gold' and ultimately 'Diamond'.[37] Advancing to higher levels of Vitality status unlocks additional perks for members, including significant discounts on travel costs.

The respondent in this case was Liberty Group Ltd, which operates in the same market as Discovery Life Ltd.[38] The core of the applicants' argument centred around Liberty's strategy of offering rebates to its clients who also participate in Discovery's Vitality programme, with the amount of the rebate being contingent upon their Vitality status.[39] The applicants challenged this practice on two fronts: (a) as a violation of their trade mark rights; and (b) as constituting unfair competition.[40] The latter claim is of particular interest for the present topic as it directly addressed the issue of Liberty's use of information linked to Discovery's Vitality programme. The applicants argued that Liberty's use of a person's Vitality status — an instance of information generated by Discovery Vitality (Pty) Ltd — was wrongful.[41]

[33] Ibid.
[34] *Discovery* supra note 22 para 1.
[35] Ibid para 3.
[36] Ibid.
[37] Ibid.
[38] Ibid paras 5 and 6.
[39] Ibid.
[40] Ibid para 8.
[41] Ibid.

https://doi.org/10.47348/SALJ/v142/i1a10

The Johannesburg High Court ruled against Discovery and its subsidiaries, holding that since members of the Vitality programme are free to share their Vitality status as they wish, Liberty's practice of offering paybacks based on this status was not wrongful.[42] The judgment implicitly drew a distinction between two categories of personal information. First, it recognised that the personal information collected by Discovery Vitality to ascertain a member's Vitality status — ranging from basic details like names and contact information to more sensitive health-related information such as medical history and biometric readings — qualifies as proprietary *confidential* information of Discovery Vitality.[43] This categorisation is supported by South African jurisprudence, which holds that confidential information, to be considered as such, must be both applicable in trade or industry and of economic value to its holder, known only to a select group rather than falling in the public domain.[44]

The second category of personal information that was considered in the judgment was members' Vitality status in Discovery's Vitality programme. The court held that an individual's Vitality status is not part of Discovery Vitality's proprietary confidential information.[45] The court explains its reasoning as follows:

> 'Vitality members pay for their membership of the Vitality programme. One of the things they get in return is their personal Vitality status. They are entitled to use this for whatever lawful reason they may wish. … The point is that members of the public, who have paid for their Vitality membership and status, should be entitled to continue to have the choice of what they wish to use that status for. … To prevent Vitality members from being able to exercise this choice would be to restrict their own proprietary interests in their Vitality status.'[46]

Thus, although an individual's Vitality status is generated by Discovery Vitality, the proprietary interest in this category of personal information does not vest in Discovery Vitality — in contrast with the other personal information that it collects about its clients — but with the individual himself or herself. And the reason is contractual: the individual Vitality member *pays* Discovery Vitality to generate this category of personal information.

The judgment in *Discovery* is a powerful repudiation of the argument by the Information Regulator in *Black Sash Trust* that a data subject is necessarily the owner of the personal information that relates to him or her. Not only are a person's proprietary rights in personal information

[42] Ibid para 97.
[43] Ibid para 68.2.
[44] Cf *Experian SA v Haynes* 2013 (1) SA 135 (GSJ).
[45] *Discovery* supra note 22 paras 68.4 and 78.
[46] Ibid paras 88–9.

https://doi.org/10.47348/SALJ/v142/i1a10

that relate to him or her contingent upon contract, but other persons can have proprietary rights in that same personal information. However, this presents what seems to be a legal dilemma: how can one person assert proprietary rights over personal information that simultaneously is subject to another person's informational privacy rights? Furthermore, how can one person's claim to proprietary rights over another person's personal information coexist with the latter person's freedom to share that same personal information with third parties? These questions appear to pose a paradox. Yet, this supposed paradox is dissected and resolved in the subsequent analysis.

It is interesting to note that the judgment in *Discovery* does not use the term 'ownership', but instead uses the term 'proprietary interest' in relation to information, or simply 'proprietary information'. The reason is not clear from the judgment. Proprietary interests can include ownership, but not necessarily.[47] Importantly, the use of the terms 'proprietary interest' and 'proprietary information' imply that personal information can, at least in certain contexts, be *property* — that is, something that can be owned.

(c) Mazetti Management Services

The last case that is considered as part of this conspectus of recent case law did not specifically deal with *personal* information qua property, but instead with information *generally* qua property. The background facts of *Mazetti Management Services* were as follows. An ex-legal advisor of two businesses, Mazetti Management Services (Pty) Ltd and Ammetti Holdings (Pty) Ltd, allegedly stole digital information from the businesses and made it available to journalists.[48] The journalists wrote an exposé on the businesses — one that was severely critical of their business dealings — and approached the businesses for comment prior to publication, whereupon the businesses insisted on the return of the relevant digital information.[49] However, the journalists refused, and alleged that the information was not in their possession, but was kept on two servers outside South Africa — although they admitted to being in control of one of these servers.[50] The businesses then approached the Johannesburg High Court on an urgent ex parte basis, inter alia for an order to compel the individual journalists and their organisation to return the digital information.[51] The order was granted as a rule nisi.[52] On the return date, the court took a dim view of the businesses' litigation tactic to approach the court on an ex parte basis, and held that

[47] *Waste Products Utilisation (Pty) Ltd v Wilkes* 2003 (2) SA 515 (W) at 573F–G.
[48] *Mazetti Management Services* supra note 23 para 8.2.
[49] Ibid paras 8.1 and 8.2.
[50] Ibid para 8.4.
[51] Ibid paras 4 and 8.9.
[52] Ibid para 4.

https://doi.org/10.47348/SALJ/v142/i1a10

it was an egregious abuse of process.[53] Moreover, the court viewed the case through the lens of the corruption that is prevalent in contemporary South Africa, and viewed the journalists' role in exposing corruption by using contraband information as 'a positive and necessary good in society'.[54] Against this background of sympathy with the journalists, and antipathy with the businesses, the court considered the question whether the information that the journalists allegedly had was susceptible to the businesses' rei vindicatio.

The court relied on the judgment in *Waste-Tech (Pty) Ltd v Wade Refuse (Pty) Ltd*,[55] decided 30 years earlier. In this case, a former employee of Waste-Tech (Pty) Ltd made copies of physical documents containing information pertaining to the company's laboratory, and supplied these copies to his new employer, Wade Refuse (Pty) Ltd. Waste-Tech (Pty) Ltd applied for an Anton Piller order. Importantly, it framed its case as the recovery of its confidential information, to which the documents containing such information were incidental.[56] In line with this approach, it did not identify the specific documents that it sought to recover.[57] Therefore, the main legal question in *Waste-Tech* was whether a proprietary right can exist in information. To answer this question, the court provided an overview of the case law at the time, and concluded that there was no basis for Waste-Tech (Pty) Ltd's argument that it had a proprietary right in its confidential information.[58] Interestingly, the court also referred to a passage in Justinian's *Institutes* that reads: 'If Titius has written a poem, a history, or a speech on your paper or parchment, you, and not Titius, are the owner of the written paper'.[59] This passage will be considered in more detail in the analysis below.

The problem with the *Mazetti Management Services* judgment's reliance on the *Waste-Tech* judgment is that the law has since evolved, and that it is doubtful whether the latter judgment is still good authority on the topic. For example, in the 2009 case of *Competition Commission v British American Tobacco South Africa (Pty) Ltd*,[60] the Competition Tribunal treated electronic point-of-sale information as something that can be bought and sold, which necessarily implies that such information is property. Furthermore, in the 2015 case of *Curemed CC v Van Onselen*,[61] where the return of confidential information was claimed, the Pretoria High Court explicitly

[53] Ibid para 11.
[54] Ibid para 24.
[55] 1993 (1) SA 833 (W) at 842H–845A.
[56] Ibid at 841D.
[57] Ibid at 837J–838A.
[58] Ibid at 839F–839G.
[59] Ibid at 843C, referring to Inst 2.1.33.
[60] [2009] ZACT 46.
[61] [2015] ZAGPPHC 176 para 29.

https://doi.org/10.47348/SALJ/v142/i1a10

held that the applicant had a proprietary interest in the information that it aimed to protect. Lastly, of course, in the 2020 case of *Discovery*, analysed above, which concerned personal information as a subset of information generally, the Johannesburg High Court held that it is indeed possible to have a proprietary interest in respect of personal information. Thus, given these recent judgments, the decision in *Mazetti Management Services*, based on the rationale of the three-decades-old *Waste-Tech* that information is not property, seems to be retrogressive, and ultimately erroneous.

The case of *Mazetti Management Services* offered an ideal opportunity for the court to engage in a thorough analysis of the ownership of information, applying the basic tenets of the common law to information in the digital age. Unfortunately, this opportunity was missed. The remainder of this article is an attempt to present such a thorough analysis.

III ANALYSIS: PROPERTY LAW AND INFORMATIONAL PRIVACY LAW

This part of the analysis commences by differentiating between *property law* and *informational privacy law* as two distinct domains of the law — each with their own different objectives and rules. It then progresses to an investigation into how these two domains interact with each other in the context of personal information.

(a) Property law

Property law governs the relationship between persons and property, and the relationship between persons with relation to property. A central concept in property law is 'ownership'. Ownership is best understood as a bundle of rights that a person — the owner — has in respect of the owned property.[62] This bundle of rights includes, most prominently, the power to use, to enjoy the fruits, to consume, to possess, to dispose, to reclaim, and to resist any unlawful invasion of the property.[63] Ownership can be encumbered in many ways, meaning that one or more of the rights entailed by ownership are partially or fully restricted.[64] Notably, ownership is hardly ever unencumbered. For example, if one is the owner of a car, one can use the car to drive to a shop, but one must do so according to the rules of the road; and one may sit on one's rocking chair on one's porch, but not throw it at the neighbour's window.

What kinds of things can be property? In other words, what kinds of things are susceptible of being owned? Our law has settled on the position

[62] *Pearly Beach Trust v Registrar of Deeds* 1990 (4) SA 614 (C).

[63] Anne Pope, Elmien du Plessis & P J Badenhorst (eds) *The Principles of the Law of Property in South Africa* 2 ed (2020) 99.

[64] C G van der Merwe 'Things' in W A Joubert (founding ed) *The Law of South Africa* vol 27 2 ed (2014) paras 136 and 139.

https://doi.org/10.47348/SALJ/v142/i1a10

that both corporeal or incorporeal things can be property, provided that they have an independent existence outside the human body, are useful and valuable, and — importantly for present purposes — are capable of human control.[65] Consider how these criteria apply to an everyday example, such as water. Can water — the ubiquitous substance found in nature, composed of hydrogen and oxygen — be owned? I suggest the answer must be a *qualified* 'yes'. Consider our planet and its vast oceans. Clearly, humans have no *control* over these colossal volumes of water, and therefore cannot stake a claim of ownership. However, if a controllable volume of water, say a litre, is taken from a fountain and bottled, it becomes (a) distinct from the rest of the water in the fountain; (b) useful and valuable (provided there is a market for water from this source); and (c) capable of human control. Therefore, the water *in the bottle* is an object that can be owned.[66] It can, for example, be sold or donated. However, what happens if you buy a bottle of water but then accidentally spill it on the pavement and it all evaporates? Although the water molecules still exist somewhere in the sky, those molecules are no longer within human control. Therefore, your water has ceased to exist as property. From a property-law perspective, the point is the water can be owned only if (and as long as) it is in a form that is capable of human control.

The next important topic to consider is how ownership is *acquired* in property. The law differentiates between the *original* acquisition of ownership and the *derivative* acquisition of ownership.[67] *Original* acquisition is when an owner acquires ownership other than from a previous owner of the property. This is usually the case when a new thing come into existence, such as a new harvest of apples. As the apples are new, they could not have been owned by anyone before coming into existence. Once they come into existence and are separated from the apple trees, the legal default position is that the owner of the orchard will be the owner of the apples. From this point onwards, the owner has the right to dispose of the property, meaning that the owner can transfer ownership of the apples to someone else. This would be *derivative* acquisition — when an owner acquires ownership from the previous owner of the property, for example if someone buys an apple from the owner of the orchard.

Before applying the principles of property law to personal information, it is necessary to first also understand the basics of informational privacy law.

[65] Pope et al op cit note 63 at 37.

[66] See Gustav Muller, Reghard Brits & Zsa-Zsa T Boggenpoel *General Principles of South African Property Law* (2019) 28.

[67] *FirstRand Bank Ltd v SMB* [2023] ZAGPJHC 904 para 25; Pope et al op cit note 63 at 161; Van der Merwe in *LAWSA* op cit note 64 para 169.

https://doi.org/10.47348/SALJ/v142/i1a10

(b) Informational privacy law

Privacy law is a domain of the law that is premised on the idea that it is necessary for one to have a personal space of seclusion from the public and publicity in order to develop and maintain one's own autonomous identity — something that is vital to one's dignity.[68] Given that one's privacy rights are intended to protect the sanctity of one's *own* personal space, one's privacy rights are inextricably bound to oneself. Unlike property rights, which are unrelated to the human personality and can therefore be transferred, privacy rights are not transferable.[69]

Informational privacy law, as a subdomain of privacy law, deals with the abstract personal space of personal information. In South Africa, this area of law was codified through the enactment of POPIA in 2013. The genesis of POPIA can be traced back to a discussion paper and draft legislation, which were prepared by the South African Law Reform Commission in 2005,[70] and followed four years later with a report and a Bill.[71] In formulating this draft legislation, the Commission drew inspiration from various pre-existing international informational privacy instruments, notably Convention 108[72] and the OECD Guidelines.[73] Given the foundational role of these international instruments, POPIA shares a familial resemblance with many other personal information protection statutes around the world, such as the GDPR, which are similarly underpinned by principles articulated in these international instruments. The operationalisation of POPIA was a phased process, culminating in its full implementation in mid-2021.[74] This narrative underscores the interconnectedness of South African informational privacy law with global privacy norms.

How does informational privacy law protect an individual's autonomy in respect of their personal information? POPIA sets out quite a number of data subject rights, including the rights (a) to have one's personal information processed in accordance with POPIA's eight conditions for processing of personal information;[75] (b) to be notified if one's personal information is being collected or has been accessed by an unauthorised person; [76] (c) to

[68] *Bernstein v Bester* 1996 (2) SA 751 (CC) paras 65–8.

[69] *Kumalo v Cycle Lab (Pty) Ltd* [2011] ZAGPJHC 56.

[70] South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005).

[71] South African Law Reform Commission Report (Project 124) *Privacy and Data Protection* (2009).

[72] Convention 108 op cit note 2.

[73] OECD guidelines op cit note 1.

[74] Proclamation R21 in *GG* 43461 of 22 June 2020 read with POPIA, s 114(1). See also Donrich Thaldar & Beverley Townsend 'Exempting health research from the consent provisions of POPIA' (2021) 24 *PER/PELJ* 1.

[75] POPIA, s 5(1).

[76] POPIA, s 5(1)*(a)*.

https://doi.org/10.47348/SALJ/v142/i1a10

establish whether a person holds one's personal information;[77] (d) to request where necessary, the correction, destruction or deletion of one's personal information;[78] (e) to object, on reasonable grounds, to the processing of one's personal information;[79] (f) to object to the processing of one's personal information for purposes of direct marketing;[80] (g) not to be subjected to automated decision-making based on one's personal information (under certain circumstances);[81] (h) to submit a complaint to the Information Regulator regarding the alleged interference with the protection of the personal information;[82] and (i) to institute civil proceedings regarding the alleged interference with the protection of one's personal information.[83]

Evidently, these informational privacy rights differ from the rights entailed by ownership. However, some informational privacy rights have characteristics that resemble the rights that are part of the ownership bundle of rights. For example, the right to have one's personal information deleted corresponds with the right of an owner to destroy the property. Also, POPIA's processing limitation condition provides that personal information may be processed only if a legal ground for processing is present. [84] One of the six possible legal grounds is consent by the data subject. Consent as a legal ground for processing can be perceived to correspond with a scenario in property law where an owner agrees to transfer the right to use the property to another person, such as in the case of a loan for use.[85]

This raises the question: do these informational privacy rights with ownership-esque characteristics give rise to ownership of the personal information to which they relate?

(c) The interaction between property law and informational privacy law

The question above must be answered in the negative. Having a characteristic that resembles an ownership right does not give rise to ownership. Thaldar & Shozi point out that 'to treat rights that emanate from ownership as indiciae of ownership is misguided, as it confuses cause with effect. For example, the right to use a thing is a consequence of ownership, not its cause.'[86] The folly of assuming ownership based on the

[77] POPIA, s 5(1)*(b)*.
[78] POPIA, s 5(1)*(c)*.
[79] POPIA, s 5(1)*(d)*.
[80] POPIA, s 5(1)*(e)* and *(f)*.
[81] POPIA, s 5(1)*(g)*.
[82] POPIA, s 5(1)*(h)*.
[83] POPIA, s 5(1)*(i)*.
[84] POPIA, s 11.
[85] See Pope et al op cit note 63 at 57 and 58.
[86] Donrich Thaldar & Bonginkosi Shozi 'The legal status of human biological material used for research' (2021) 138 *SALJ* 881.

https://doi.org/10.47348/SALJ/v142/i1a10

observation of ownership-esque characteristics can be further illustrated by the following example: everyone has the right of self-defence if someone threatens one's bodily integrity, which resembles the ownership right to resist unlawful invasion of one's property. However, this does not mean that one owns one's body — at least not in the legal sense. One's body is part of one's legal personhood, not one's estate. Whether an object can be owned is determined by the relevant *property-law* rules (having an independent existence outside the human body, being useful and valuable, and being capable of human control),[87] and not by exhibiting a characteristic that resembles one or more ownership rights.

Similarly, after establishing that an object can be owned, the relevant *property-law* rules must be applied to determine who the object's owner is. Consider the following example: if you see a person driving a red sports car, can you, without more information, conclude that the person is the *owner* of the red sports car? The answer is clearly 'no'. The person *may* be the owner, but there are other possibilities, such as the person is borrowing or renting the car from its owner — both reasonable and lawful possibilities. If there is a contract of loan for use, or a contract of lease, the right to use the sports car is transferred from the owner to the borrower or the renter. The ownership of property is determined by the property-law rules of acquisition of ownership discussed above, combined with other branches of the law — most notably contract law — and not by spotting the exercise of rights that are characteristic of ownership but that are not exclusive to it.

It should now be clear why the argument advanced by the Information Regulator in *Black Sash Trust* was misconceived. Informational privacy rights may have characteristics that resemble ownership rights, but this observation per se does not necessary mean that personal information can be owned, or that data subjects own their personal information.

IV ANALYSIS: THE APPLICATION OF PROPERTY LAW TO PERSONAL INFORMATION

This part of the analysis addresses whether personal information can be owned and, if so, by whom. As concluded in the previous part, these questions must be answered by applying the relevant rules of *property law*. Given that we find ourselves in the digital age, the analysis concentrates on the impact that the digitalisation of personal information has in the property law context. The analysis then returns to the interaction between property law and informational privacy law in the context of personal information. This sets the stage to resolve the supposed paradoxes posed by the *Discovery* judgment.

[87] Pope et al op cit note 63 at 37.

https://doi.org/10.47348/SALJ/v142/i1a10

(a) Whether personal information can be owned

Is personal information susceptible of ownership — can it be property? I suggest a *qualified* affirmative answer. Similar to the example of water above, which is often not within human control — think of the oceans and the clouds — personal information becomes susceptible of ownership only if it is brought within human control.[88] However, the control of personal information may often be elusive. For example, my memories about my life would — to varying degrees of vagueness or clarity — be accessible to my conscious mind but are not capable of human control generally speaking and, accordingly, my memories about my life are not susceptible of being owned. However, just like water that can, for example, be bottled to bring it within human control, personal information can be *recorded*. If, for example, the security cameras in my home digitally record a certain event in my life, the details of this event are not only precariously stored in the neurons of my brain but are also stored as a digital video recording. This video recording has an independent existence outside the human body, can be useful and valuable, and is capable of human control. Evidently, the video recording is susceptible of being owned — it is *digital property*.

In the same vein, when exploring how property law applies to genomics research, my colleagues and I have proposed that the most promising unit of (property-law) analysis of genomic information is an *instance* of the information, meaning a computer file — a digital property — containing the information.[89] I suggest that this insight in the context of genomic information is applicable to personal information generally. It highlights that a conceptual distinction must be drawn between the personal information *in general*, and a specific *instance* of such personal information. While the former is not within human control, the latter is indeed within human control.

An important corollary of this distinction is that owning an instance of personal information does not necessarily mean that one owns such personal information generally. It also follows that different instances (or copies) of the information can be owned by different persons. However, if all instances of the relevant personal information are owned by a single person, and no one is alive who knows or is able to recall the relevant personal information, that person could be deemed *effectively* to own the relevant personal information in general.

In practical terms, being the owner of the video recording of the event at my home will entitle the owner to exercise all the typical powers of

[88] Pope et al op cit note 63 at 39.
[89] Thaldar et al op cit note 11.

https://doi.org/10.47348/SALJ/v142/i1a10

ownership in respect of the video recording — subject to my privacy rights, as I analyse below. Examples of such powers of ownership are claiming it back from anyone who is in unlawful possession of it, or selling the video recording.[90] It also means that if the video recording is unlawfully copied, the culprit will be committing a *property* crime — theft. Notably, the Cybercrimes Act 19 of 2020 provides that the common-law offence of theft must be interpreted not to exclude the theft of incorporeal property.[91] As the definition of theft requires that the relevant stolen object must be owned by someone, this provision of the Cybercrimes Act necessarily implies that incorporeal property, such as personal information, can be owned.[92]

Interestingly, the unlawful copying of a video recording was indeed the topic of the *Dixon* case in New Zealand.[93] The facts, in brief, were as follows. A nightclub's closed-circuit television ('CCTV') camera recorded a (married) celebrity sports star interacting with a female patron (who was not his wife).[94] A bouncer working at the nightclub thought that this was an opportunity to make money. He surreptitiously copied the digital files containing the CCTV footage from the nightclub's computer to his memory stick, deleted the original files from the nightclub's computer, and attempted to sell the digital files to the media.[95] However, it did not end well for the nightclub bouncer. Not only did he fail to sell the files to anyone, but he was criminally prosecuted and convicted of the statutory offence of accessing a computer system for a dishonest purpose to obtain property.[96] New Zealand's Supreme Court held that digital files are indeed susceptible of ownership and thus qualify as property for the purposes of the statutory offence.[97]

In conclusion, by recording personal information, it enters the realm of property law as an thing that can be owned — property. But, *who* owns such property? It is important to remember that this is a *property-law* question. In contrast with informational privacy rights, which attach in a person based on a personal connection with the object of the rights, such a personal connection is irrelevant for purposes of determining ownership.[98] In part IV(b), I explore how property-law rules apply to the question of who owns an instance of personal information, such as a video recording.

[90] See for discussion on the common-law remedy of rei vindicatio (recovery of property by owner) Pope et al op cit note 63 at 210.

[91] Section 12 of the Act.

[92] For the definition of theft see C R Snyman *Criminal Law* 6 ed (2014) 475 as cited in *Mdebuka v S* [2020] ZAFSHC 131 para 12.

[93] *Dixon v R* [2015] NZSC 147, [2015] 27 CRNZ 593.

[94] Ibid para 1.

[95] Ibid para 2.

[96] Ibid para 3.

[97] Ibid paras 51–4.

[98] Thaldar op cit note 12.

https://doi.org/10.47348/SALJ/v142/i1a10

(b) Determining the ownership of personal information

In the conspectus of recent case law above, the following passage from the *Corpus Juris Civilis* was quoted: 'If Titius has written a poem, a history, or a speech on your paper or parchment, you, and not Titius, are the owner of the written paper.'[99] This principle still applies centuries later. When information is recorded by writing it down in a book, the owner of the book remains the owner of the book, which now simply includes an instance of the information. However, in our digital age, information is typically recorded digitally. This raises the following question: when personal information is recorded by saving it on a device such as a computer or a cell phone, would the owner of the device not automatically be the owner of the instance of the personal information? Although this may seem like an attractive solution, it is not. The reason is that it fails to account for the different ways in which we humans experience our interaction with the physical world and the digital world. I explain this reason by first analysing the general principle of how property law conceives of property, and then I apply the analysis to the digital world.

The law needs to govern human activity practically. Therefore, the legal conception of property should reflect the typical human experience of interaction with their environments. Consider for example the book mentioned in the paragraph above. A book is legally conceived of as a single item of property, rather than the ink and the paper being separate property, or each molecule of the book being a distinct item of property, or the vast number of carbon, hydrogen and oxygen atoms that a book is composed of each being separate property. This is because a book is the relevant unit with which we humans interact in the normal course of our daily activities.

In the digital age, we humans interact not only with corporeal property and traditional incorporeal property, such as an inheritance, but also with a new kind of incorporeal property, namely *digital property*. Everyday examples of digital property would be digital money, word-processor documents and email messages. Digital property may often contain personal information — think of digital photos, video clips, electronic health-record files, and computer files containing human genomic sequences. We transfer money electronically to our creditors, send photos to our friends and family on social media, email word-processor files to colleagues, and make genomic information files available for online analysis in trusted research environments. Even though our interaction with the digital world is mediated by devices in the physical world, and property in the digital world also has a physical presence where it is recorded, such

[99] Inst 2.1.33.

https://doi.org/10.47348/SALJ/v142/i1a10

as on one's device and on the cloud (meaning on various computer servers located all over the planet), the relevant object of our interaction with the digital world — as dictated by typical human experience — is the digital property. To illustrate, when I transfer pocket money to my teenage son's bank account using the banking app on my cell phone, my son and I both conceive of the transaction as money in the digital world being transferred from one account to another. We do not think of the transaction in physical terms as me initiating a reordering of binary code on the bank's computers' silicon chips.

Accordingly, when information is recorded by saving it as a new file on a device (or devices), what is relevant from a property-law perspective is that new property is created in the digital world. The fact that existing property in the physical world, such as a cell phone or computer servers in the cloud, is physically altered (in a way that is imperceptible to the human eye) to house the new file in the physical world is, I suggest, incidental and of no consequence from a property-law perspective.

A prime example of the legal significance of digital property is the Dutch RuneScape case.[100] RuneScape is an online game where a player plays a character in a fantasy virtual world. Two boys (the accused) used violence in the real world to force a third boy (the victim) to log into his RuneScape account and (in the virtual world) to drop his character's amulet and mask for the character of one of the other boys to take. Is this theft — can one steal an object that exists only in a virtual world? The accused boys' legal representatives adopted an exclusively physical-world approach, arguing that the virtual objects were nothing more than bits and bytes — mere information — and not property that can be stolen. However, the courts did not agree. The trial court, the court of appeal and, ultimately, the Hoge Raad (the apex court in the Netherlands) all found the accused boys guilty of theft. The Hoge Raad held that the test for assessing whether something qualifies as property that can be stolen is whether it has value for the person involved. Because the virtual amulet and mask clearly had value for the boys, these virtual objects qualified as property for the purposes of the case. In other words, the law adapts to the way in which the persons involved experience their interaction with the world — including the digital world. The judgment not only confirmed that digital property can be owned, but also that acquiring ownership of property in the digital world is determined in the context of the digital world — not by ascertaining where the bits and bytes are stored in the physical world.

[100] ECLI:NL:RBLEE:2008:BG0939, Rechtbank Leeuwarden, 21 October 2008; ECLI:NL:GHLEE:2009:BK2773, Gerechtshof Leeuwarden, 10 November 2009; ECLI:NL:PHR:2012:BQ9251, Hoge Raad, 31 January 2012.

https://doi.org/10.47348/SALJ/v142/i1a10

I now return to the (inapt) analogy between recording information in a book and a device. The reason the analogy breaks down is that in the case of the device the act of recording information opens up a new echelon of interaction — the digital world — between the human subject and the information. This new echelon of interaction is not available in the case of the book. Moreover, this new echelon of interaction becomes the defining paradigm in which the human subject interacts with information. In the digital world, information that is newly recorded is new property. To illustrate this, if one takes a photo with one's cell phone, a new image file — new digital property — comes into being. Similarly, if a laboratory technician sequences a person's DNA, a genomic information computer file — new digital property — comes into being.

As discussed in part III above, if new property comes into being, the rules of *original* acquisition of ownership must be applied. Original acquisition of ownership can transpire through one of a numerus clausus of modes of original acquisition.[101] Which mode applies depends on factors such as the nature of the property (for example, a piece of treasure) and the way in which it has come into being (for example, by manufacturing it from antecedent property). Now, consider a new digital information instance. It comes into being when information is digitised — that is, digitally recorded. In other words, its antecedent is the information in a pre-recorded state. However, information in a pre-recorded state is not property. Therefore, from a property-law perspective, a new instance of digital information is without antecedent. It is res ex nihilo — something out of nothing. This eliminates original modes of acquisition such as manufacture (where a person manufactures a new product from the antecedent property of others) and the acquisition of fruits (where an antecedent fruit-bearing property, like a fruit tree, produces new property, the fruit) that rely on the existence of antecedent property. The only reasonable possibility is that a new digital information instance starts its legal existence as being owned by no one — res nullius — and that the applicable original mode of acquisition is appropriation.[102] Appropriation applies to situations where a person brings a res nullius under his or her control with the intention of owning it. In other words, when a new digital information instance is generated, the first person who intends to own it and who effectively controls it becomes the owner.[103]

This property-law conclusion can be combined with the law of agency, providing that a person can act as someone else's agent in appropriating the new digital information instance and that is combined in innumerable ways

[101] Pope et al op cit note 63 at 163.
[102] See Thaldar et al op cit note 11; Thaldar op cit note 12.
[103] Both sources ibid.

https://doi.org/10.47348/SALJ/v142/i1a10

with the law of contract to ensure a consensus-based ownership outcome between all parties involved in the generation of a new instance of digital information.[104] For example, to use the example of the video recording at my home, I can agree with the company that installs the security cameras that all video recordings will be on its cloud server (within their control, not mine), but that I will be the owner thereof, meaning that the company will exercise control on my behalf. This aligns with the *Discovery* judgment, where the court held that although Discovery Vitality generates a Vitality member's Vitality status, the member has proprietary interest in his or her Vitality status by virtue of paying a membership fee to the Vitality programme that includes having a Vitality status.

(c) Redux: the interaction between property law and informational privacy law

It bears repetition that a personal connection between a person and property is not relevant in determining ownership. Therefore, none of the modes of acquisition of ownership pay any regard to such a personal connection. However, the situation is different in informational privacy law, where a data subject enjoys rights in personal information by virtue of the fact that such information relates to and identifies him or her. Is the ownership position sketched above not a recipe for conflict between personal information owners (persons who own instances of personal information) and the data subjects to whom such personal information relates?

Whenever different persons have rights (originating in different branches of the law) in respect of the same property, these rights can come into conflict. This is not a new problem, and the law has over the centuries developed rules to resolve such conflicts — primarily through rules that determine which rights will take precedence in which circumstances. In the case of informational privacy rights versus ownership rights, the way to resolve conflict is clear: as a general rule, statute law overrides common law,[105] and since informational privacy rights are codified in statute (POPIA) while ownership rights are based in common law, informational privacy rights supersede ownership rights to the extent that they are in conflict in any given situation.[106] In other words, the personal information owner's (common-law) rights are restricted by the (statutory) rights of the data subject. This means that the personal information owner would be able to process the personal information, such as licensing the information to a third party, only in a way that is consistent with the obligations imposed

[104] See Pope et al op cit note 63 at 79.

[105] Lirieka Meintjes-van der Walt (ed) *Introduction to South African Law: Fresh Perspectives* 3 ed (2019) 146.

[106] Ibid.

https://doi.org/10.47348/SALJ/v142/i1a10

by POPIA,[107] which may require the data subject's consent, depending on the circumstances.[108]

It is useful to consider the concept of a personal servitude. A personal servitude gives its holder a limited real right over the res serviens. This means that the rights entailed by the personal servitude can be enforced against anyone, not only the current owner of the res serviens.[109] A personal servitude is different from other real rights, such as ownership and praedial servitudes, because it is, as the name suggests, personal in nature and hence non-transferable and extinguishes at the holder's death. There is no numerus clauses of personal servitudes, and new types can be created through agreement or statute[110] — or even through prescription or a court order.[111] I suggest that a data subject's informational privacy rights, to the extent that they encumber ownership of a personal information instance, constitute a new species of personal servitude in property law.

An interesting and unique aspect of this new species of personal servitude is that it can be extinguished if the personal information owner de-identifies the information. This entails the removal of the personal connection between the data subject and the information instance and causes POPIA to cease applying to the information.[112] However, de-identification is not always possible or desirable. For example, in certain research projects, having 'high resolution' geospatial information would yield more accurate results, but would also increase the likelihood that data subjects could be identified. In such cases, owners of digital information instances may prefer not to attempt to de-identify the personal information, hence preserving the data subjects' personal servitudes and remaining subject to POPIA's prescripts.

(d) Resolving the paradoxes

The analysis illuminates how to untangle the supposed paradoxes that were revealed by the *Discovery* judgment. Consider the first perceived paradox: how can one person assert proprietary rights, such as ownership, over personal information that simultaneously is subject to another person's informational privacy rights? The key to resolving this apparent contradiction is the principle that multiple branches of the law can apply to a single object, producing distinct and sometimes competing rights

[107] POPIA, chap 3: Part A.
[108] POPIA, s 11.
[109] *Stoch v Mntambo NO* [2022] ZAGPJHC 544 para 64; Pope et al op cit note 63 at 229.
[110] Pope et al ibid.
[111] *Stoch* supra note 109 para 62.
[112] POPIA, s 6(1)*(b)*.

https://doi.org/10.47348/SALJ/v142/i1a10

regarding that object. When informational privacy rights conflict with ownership, the former take precedence due to their statutory basis, as opposed to the common-law basis of the latter, effectively resolving the issue.

The second supposed paradox is: how can a firm's claim to proprietary rights over a client's personal information coexist with the client's freedom to share that same personal information with third parties? The firm's proprietary claim is confined to a *specific* instance of the personal information, and does not include the client's personal information in *general*. This delineation ensures that the client retains the ability to share the same personal information with third parties, unfettered by the firm's proprietary claim over the specific instance of the personal information in its possession. Viewed from this angle, the *Discovery* judgment is solidly supported by legal theory.

V CONCLUSION

From a pre-digital age perspective, the digital world seems magical. New digital property is created from nothing — it is like a new parchment scroll appearing in a mage's library when he snaps his fingers. And, at a second snap of his fingers, exact copies of the scroll can appear on the desks of other mages in far-flung corners of the world. But this is exactly what happens when we compose emails or take video clips of our activities and send them to our friends and family in far-flung corners of the world using social media. This observation is at the core of my suggested approach to personal information ownership. If we accept the jurisprudential stance that the legal conception of what constitutes property should reflect the typical human experience of interaction with the world, it follows that because, in our digital age, we humans constantly interact with *digital property* — whether digital photos, video clips, word-processor documents or genomic sequence files — *they*, rather than the physical devices on which they are recorded, are the relevant property when considering personal information ownership. This determines how ownership is acquired in personal information, in particular the res nullius construction of a new digital information instance.

Kish & Topol suggest that transactions involving information become trusted when the ownership thereof is clear.[113] This underlines the need for legal clarity on information ownership — in particular, the ownership of *personal* information, given that the ownership-esque nature of some informational privacy rights seems to befuddle some legal minds. An instance of personal information can indeed be owned, but it is not

[113] Leonard Kish & Eric Topol 'Unpatients — Why patients should own their medical data' (2015) 33 *Nature Biotechnology* 921.

https://doi.org/10.47348/SALJ/v142/i1a10

necessarily owned by the data subject. The person best positioned to acquire ownership of personal information is the person on whose device the new information is recorded, as this person is in control of the personal information from the outset and therefore only needs the intention to be the owner of the personal information to acquire ownership of it in law. That said, the acquisition of ownership of a new personal information instance can be contractually arranged, which opens the door to many scenarios. Importantly, the recognition that ownership of a personal information instance can be acquired by someone other than the data subject is not a legal anomaly. It simply means that ownership of such a personal information instance is encumbered by the informational privacy rights of the data subject.

The Chinese government, acknowledging the need for clearer and more effective regulations regarding data usage, recently issued a new policy that is focused on the commercialisation of data.[114] (To maintain precision in alignment with the original Chinese terminology, the term 'data' is used, rather than 'information'.) This policy aims to harness fully the potential of data as a key production factor, and comprehensively provides for rights in data, including personal data. Interestingly, at a foundational level, this policy is remarkably similar to the position in South African law that I have sketched in my analysis above. In particular, the policy draws a clear conceptual distinction between privacy rights and property rights, and provides that while data subjects have privacy rights in the personal data that relate to them, they do not necessarily have property rights in them. The policy, like South African law, provides that privacy rights are first-order rights that supersede property rights in the same personal data. The main difference between the Chinese policy and the South African position is that the Chinese policy-makers did not refer to 'ownership', and instead opted to provide for a number of specific property rights in data that are intended to function in a modular fashion. However, these data property-rights modules created in the Chinese policy — the rights to hold, use and manage the data for profit — are for all practical purposes identical to some of the rights in the traditional ownership bundle of rights. The Chinese policy proceeds to develop sophisticated rules to deal

[114] 中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见, translated into English as Opinions of the CPC Central Committee and the State Council on Establishing a Data Base System to Maximize a Better Role of Data Elements (2022), available at *https://www.pkulaw.com/en_law/1b51343d19be0d11bdfb.html,* accessed on 20 April 2024. For a discussion of this policy see Bingwan Xiong, Jiangqiu Ge & Li Chen 'Unpacking data: China's "bundle of rights" approach to the commercialization of data' (2023) 13 *International Informational Privacy Law* 93.

https://doi.org/10.47348/SALJ/v142/i1a10

with conflicts between the rights of different property rights holders. In this sense, the Chinese policy is undoubtedly leading the world.

The economist Hernando de Soto noted from an historical perspective that '[t]he moment Westerners were able to focus on the title of a house and not just the house itself, they achieved a huge advantage over the rest of humanity'.[115] This is because people could go beyond thinking about their assets as they are (houses used only for shelter) to thinking about what they could be (security for credit to start or expand a business), hence creating more economic opportunities. I suggest that the same rationale applies to personal information and the ownership thereof. To actualise the economic potential of information — the fuel of the digital economy — fully, countries worldwide should actively seek to clarify the nature of ownership of personal information.

[115] Hernando de Soto 'The hidden architecture of capital' Peruvian Institute for Liberty and Democracy research paper (2001), available at *http://www.ild.org.pe/publications/articles/863-the-hidden-architecture-of-capital*, accessed 7 September 2023.

https://doi.org/10.47348/SALJ/v142/i1a10