Privacy by design: a Holochain exploration

Kirsten Wahlstrom
University of South Australia,
Australia
Kirsten.Wahlstrom@unisa.edu.au

Anwaar Ulhaq
School of Computing and Mathematics,
Charles Sturt University,
Australia

Oliver Burmeister
School of Computing and Mathematics,
Charles Sturt University,
Australia

Abstract

Privacy is important because it supports freedom, dignity, autonomy, justice, and democracy, and therefore it is important that privacy is studied in ontologically robust ways. A form of privacy is implemented in the right to be forgotten, which is a human right established by the European Court of Justice. Blockchain and Holochain are examples of recently emerged technologies that were shaped by, and are now shaping of, social contexts in which economic transactions may occur. The right to be forgotten represents a compliance challenge for public and private implementations of blockchain technology. This paper describes a few of these challenges.

Keywords: Holochain, blockchain, privacy by design, ethics, crypto

1 Introduction

The role of privacy in information systems (IS) design has been well established in numerous domains, including the one that is the focus of this paper, namely the blockchain (Hackius, Reimers, & Kersten, 2019; Zyskind & Nathan, 2015). Information management and governance, ensuring data is tamper proof and managing business risks related to privacy have created challenges for many companies, because information is seen as a strategic asset. A blockchain is a tamper-proof and distributed data repository that supports information management and governance through automating trust, thereby reducing transaction costs; for these reasons, blockchain technology is of advantage in business (Vovchenko, Andreeva, Orobinskiy, & Filippov, 2017). However, blockchains suggest challenges for privacy and the aim of this paper is to explore some of these challenges.

Privacy has been conflated with security and confidentiality (Mittelstadt, Fairweather, McBride, & Shaw, 2013; Wahlstrom & Fairweather, 2013) and this ontological vagueness obscures all three concepts and curtails clarity in research. In this paper, a clear definition of privacy enables us to establish a stronger position on privacy with respect to the blockchain, utilising the example of Holochain.

Privacy is important because it supports freedom (Hull, 2015), dignity (Panichas, 2014), autonomy (Nissenbaum, 2004), justice (Introna, 2000), and democracy (Schwartz, 1999).

Westin considers that "… privacy is a quality of life topic worth the best scholarship, thoughtful advocacy, and continuing attention of us all" (2003, p451). The literature on privacy encompasses diverse themes (Wahlstrom, Fairweather, Ashman, & Istance, 2013): control of data and self-determination (Bernoth, Dietsch, Burmeister, & Schwartz, 2014; Westin, 1967) restricting access to self and data (Moor, 1990), privacy and data as commodities that may be traded (Posner, 1977), privacy as a social good differing from context to context (Burmeister, Islam, Dayhew, & Crichton, 2015; Dix, 1990), and the view that privacy takes shape according to the technologies forming the infosphere (Floridi, 2005).

Data privacy has been seen as distinct from physical privacy and while the distinction affords analysis (Stahl, Timmermans, & Mittelstadt, 2016), it obscures the foundation of privacy: social context. As Parent put it, "a lonely man isolated on a desert island could hardly be expected to cherish his privacy. So, we serve no useful or constructive purpose in ascribing it to him" (1983, p349). It is social context that gives rise to meaningful privacy, regardless of whether that context is the blockchain or in a grocery store. Here, privacy is understood to be an intrinsic and pliant feature of social contexts, shaped by social contexts and to a lesser extent, shaping of social contexts (Burmeister, 2016; Burmeister & Kreps, 2018; Teipel et al., 2016; Wahlstrom, Fairweather, & Ashman, 2017) and therefore we define privacy as

> *Privacy is a highly contextual social good which is instrumental to the perpetuation of other social goods. People exercise privacy through personal information preferences and practices which are specific to social contexts and changing over time.*

This view is consistent with those held by others. Gavison states "My purpose is to point out the many contexts in which privacy may operate ..." (1980, p444). One of three elements in Solove's work on conceptualising privacy is "a recognition of context and contingency" (2002, p1127) and in a later paper, Solove considers the question "How can privacy be addressed in a manner that is non-reductive and contextual, yet simultaneously useful in deciding cases and making sense of the multitude of privacy problems we face?" (2006, p481). Finally, Nissenbaum (2009) details a framework for revealing the integrity of privacy within specific contexts.

According to Panichas (2014, p159), "Privacy has undeniable implications for persons' abilities to define themselves and to command the requisite degree of respect for their dignity and autonomy." The right to be forgotten is a human right established when the European Court of Justice ruled against data controllers in Google v Spain[1]. Today, the right to be forgotten exists in Europe and Argentina. It acknowledges that one's conduct in one social context ought not to impact on one's success in other social contexts. For example, youthful drunkenness ought not to damage future access to employment opportunities. The right to be forgotten may require data controllers to remove data from indexes. Therefore, the right to be forgotten supports privacy in online contexts.

Similarly to privacy, socio-technical IS has features of social contexts, perhaps not as pliant as privacy, but shaped by social contexts and shaping of social contexts. The bitcoin blockchain is an example of technology that was shaped by (and is now shaping of) social contexts in which economic transactions occur.

[1] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González

2 Limiting privacy through a Blockchain

Blockchain is considered as a data structure that can provide the capabilities of a ledger with three main properties (Pass, Seeman, & Shelat, 2017):

1. Consensus: All participants must be agreed on what data should reside on blockchain
2. Persistence: once data has been added to the blockchain it can never be removed and
3. Liveness: anyone can add data to the blockchain and it is not possible to prevent anyone from writing new data so system can never get stuck.

Blockchain was originally intended to digitally timestamp documents to make them tamper-proof. Blockchain is considered a transparent, time-stamped and decentralized system as it provides digital trust by recording information in a public space and is tamper-proof (Carlozo, 2017). In a blockchain, a block is a cryptographic hash of the previous block's identifier, a timestamp, and transaction data (Zheng, Xie, Dai, Chen, & Wang, 2017). When a new block is added, it encapsulates the previous block and is itself later encapsulated by subsequent blocks (Zheng et al., 2017). This ensures all blocks in a blockchain are in accord; blocks may be added to the ends of a blockchain, but once added, blocks are immutable (Asharaf & Adarsh, 2017). In other words, a blockchain can be added to and read, but it cannot be amended. If it were possible to change a block, the entire chain would fail because the block's encapsulation would no longer accurately represent the previous and subsequent blocks in the chain. Therefore, data cannot be changed within or removed from blockchains.

One of the major issues with blockchains is the lack of privacy of transaction data. One of the primitive requirements is to prevent double-spending attacks (Joshi & Mathew, 2018). To do that, a user is required to reveal some information for authentication. Each computer on the network receives a record of every single transaction and update, and each computer validates these transactions. The transactions contain information like sending account, receiving account, amount, and any other details that are required for validation. In some applications, it is not acceptable for all transactions to be revealed to all participants in real time. These problems are motivating privacy as an emerging research topic in the study and development of blockchain technology.

Let us review privacy concerns in the context of bitcoin financial transactions in between two business parties and review how solutions to such concerns are evolving in with respect to blockchain technology. So, if we look at initial way of bitcoin transactions, we can see the source addresses are written on the blockchain as well as the all the amounts, and information about payer and payee. Even though due to cryptology, it is directly difficult to figure out the physical identify associated with these addresses, there are companies that analyse the blockchain and map these addresses to physical entities. It is a problem for business payers, payee and amounts are revealed, making the blockchain less trusted for business payments. For instance, if costs in supply chain are known to everyone, a business cannot gain a competitive advantage.

One idea to deal with such privacy concerns is confidential transactions (Noether & Mackenzie, 2016). The idea is rather than writing amounts in the clear, system can replace amounts with commitments to the amount. A commitment is a way to represent data in a way that no one knows what the data is but the person who wrote the data no longer can modify it. So, they are committed to a particular value.

Even though no one knows what the value is: Like Pederson commitment (Metere & Dong, 2017): Commit(v)=gv.hr where, r is random. We put value v as an exponent and we blind it by random r. Unfortunately, we lose the opportunity to verify the transaction. Normally, when we verify, we check whether the number of inputs is equal to the number of outputs in a transaction plus the fee for the miner. However, a solution named zero knowledge proof (Pass, 2019) is used to counter it. It means that payee attaches zero knowledge proof to the transaction. Some blockchain systems like zcash (Hopwood, Bowe, Hornby, & Wilcox, 2016) and Monero (Möser et al., 2018) have implemented transactions where not only the amount is hidden but also payee and payer information is hidden. Such systems use techniques such as ZnSNARK (Bitansky et al., 2017).

The right to be forgotten enshrines a legitimate right to request that personal information be erased from the Internet, so that it cannot be found by search engines. In contemporary digital history, it is associated to the case of Google Spain SL, Google Inc for request by Mario Costeja González. In the 1990s, González had financial debts that were reported by an online newspaper and later resolved. Years later, González requested his past to be forgotten, but the internet would not forget. On May 2014, the European Court of Justice ruled that Google had an obligation to remove links to González's personal data that was no longer correct (Cellan-Jones, 2014). It led to the European Union law referred to as the right to be forgotten. However, it has serious implications for corporate burden and access to information. After this decision, Google received 41,000 requests for data to be forgotten and in 2015, requests were reported to be around 1,000 a year (Laursen, 2015). In response, Google has removed various URLs from its search results.

The right to be forgotten is a perpetual burden on corporate resources and is considered very hard in implementation terms. It also suggests questions regarding the scope of European law at global scale. Finally, it highlights the enduring tension between privacy and utility, as it invites consideration of whether the benefits of privacy outweigh the costs to web indexing organisations. While the outcome of such consideration is a clear 'yes' in the deliberations of the European Court of Justice, the question remains open in other jurisdictions.

Blockchain enables the decentralised web by relying on a network of computers for distributing data (Mougayar, 2016). Each computer can act as a node, with power and memory on a distributed storage network system. The data is not stored in any one storage and therefore there is no central point to hack and control. This peer-to-peer infrastructure model of nodes is similar to a blockchain's distributed ledger and therefore it could be the answer to create a decentralized web. If we reimagine the right to be forgotten, it becomes highly infeasible from the implementation point of view. One reason is the highly decentred nature of the next generation of the Internet as no one would have the central authority on data. As a data controller (e.g., a node in a public blockchain) makes personal data public, exercise of the right will also place responsibility upon a node to take reasonable steps, to inform other controllers of any erasure request. To comply with this responsibility, data controllers will have to take all technical measures based on the available technology and the cost of implementation. In similar terms, other world states are contrary to the right to be forgotten like United States and Australia where access to the information is considered linked to the free speech and freedom (Bennett, 2012).

3 Holochain privacy

There have been various suggestions for supporting privacy (Wahlstrom, Roddick, Sarre, Estivill-Castro, & deVries, 2006), including attempts to leverage blockchain technology to provide privacy (Zyskind & Nathan, 2015). One such attempt is Holochain, which provides "Individual authority over data sharing, access, and storage" (Holochain, 2020).

Holochain is a platform for which apps (called hApps) are developed (Holochain, 2020). hApps provide for various distributed and transparent economic exchanges of value and examples include energy trading, farm produce trading, village resource-sharing, agile project management, publishing, heterogeneous IoT, social media, and event and disaster management[2]. In other words, Holochain enables distributed, server-less apps running on devices with localized data storage and management. For this reason, Holochain is disruptive of client/server platforms and cloud technologies.

A hApp "… consists of a network of agents maintaining a unique source chain of their transactions, paired with a shared space implemented as a validating, monotonic, sharded, distributed hash table (DHT) where every node enforces validation rules on that data in the DHT as well as providing provenance of data from the source chains where it originated" (Harris-Brown, Luck, & Brock, 2018, p4). In less compact terms, in a hApp each node creates its own (small) blockchain for holding verified data which is shared to a DHT (Frahat, Monowar, & Buhari, 2019). The DHT is sharded and distributed back to the nodes in the hApp (Holotescu & Vasiu, 2020), which validate the shards against their source blockchains (Harris-Brown et al., 2018).

An inherent limitation of any blockchain is its computation and communication cost, which makes a blockchain less efficient (slower) as it gets bigger. A hApp is more scalable than a blockchain because validating shards of DHT at nodes is a more efficient validation process than validating an entire blockchain. As a blockchain gets bigger, it gets less efficient and more resilient; but as a hApp gets bigger, it gets more efficient and more resilient.

Nodes in a hApp may be controlled by agents, and an agent may be a person. In this way, Holochain does indeed support "individual authority of data sharing, access, and storage." Also, Holochain transfers power from centralised data controllers such as Facebook to individual agents.

However, authority over data sharing, access, and storage is not always consistent with privacy. According to the definition of privacy adopted in this paper, privacy may take different forms in different contexts. For example, in one such context, authority over data sharing may be a privacy preference and practice for many people, but not others. In another context, authority over the sharing of sensitive data may not be practicable; for example, when a patient loses consciousness they can no longer exert authority over the sharing of sensitive data related to their health, yet it may be in the patient's best interest that the data is shared. Finally, there are many social contexts in which someone's privacy preferences and practices dictate that their authority over data sharing be waived (e.g. communications within an intimate relationship that two people share may be controlled by both parties together rather than one or the other).

[2] These and other examples are listed at https://forum.holochain.org/c/projects/7

As it is impossible to specify the privacy preferences and practices for every social context, so it is impossible to precisely state that Holochain provides privacy. However, it is clear that Holochain supports privacy for a subset of social contexts. The contexts in this subset are to be determined by Holochain's users as they develop and use hApps. For this reason, we suggest that it will be one of many privacy tools deployed by those with an interest in exercising their privacy preferences and practices.

4 Holochain privacy and the right to be forgotten

One form of privacy which is likely to be consistent with Holochain's features is the right to be forgotten. This right applies to data indexed by search engines, that is, it applies to the web.

If a search engine indexed Holochain nodes, then the data returned to web search queries would be under the control of the Holochain agents. In cases where the agent is an individual person who wants to exercise the right to be forgotten, they may re-create the small blockchain at their own node making sure to prevent the sharing of the data which is to be forgotten. Then, the agent's small blockchain is re-shared with the Holochain's DHT, which is re-sharded, and re-distributed to the nodes for verification.

If such a Holochain web search engine existed, its computational and communication costs are likely far less than a blockchain deployed for this purpose. However, these costs would be greater than we observe in today's web search engines. Our point remains that a Holochain platform is consistent with the right to be forgotten.

5 Conclusion

Privacy needs to be studied in an ontologically robust way, in relation to blockchain and in relation to any other technology or social context. It is important because it is mutually shaping of freedom, dignity, autonomy, justice, and democracy. It encompasses diverse themes including the control of data and self-determination, restricting access to self and data, privacy and data as commodities that may be traded, privacy as a social good differing from context to context, and the view that privacy takes shape according to the technologies forming the infosphere. Blockchains are technologies that were shaped by, and are now shaping of, social contexts in which economic transactions occur. As noted above, Holochain is disruptive of client/server platforms and cloud technologies. Whether Holochain's data control and computational advantages are sufficient to disrupt data is the new oil business models is a matter of conjecture, but for privacy, Holochain hApps offer significant advantages over blockchains. Privacy and data protection laws around the world represent a real compliance challenge for public and private distributed implementations of blockchain technology; and Holochain platforms have the potential to meet these challenges.

References

Asharaf, S. & Adarsh, S. (2017). *Introduction to Blockchain Technology Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities* (pp. 10-27). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2193-8.ch002

Bennett, S. C. (2012). The right to be forgotten: Reconciling EU and US perspectives. *Berkeley J. Int'l L.*, 30, 161.

Bernoth, M., Dietsch, E., Burmeister, O. K., & Schwartz, M. (2014). Information management in aged care: cases of confidentiality and elder abuse. *Journal of Business Ethics*, 122(3), 453-460.

Bitansky, N., Canetti, R., Chiesa, A., Goldwasser, S., Lin, H., Rubinstein, A., & Tromer, E. (2017). The hunting of the SNARK. *Journal of Cryptology*, 30(4), 989-1066.

Burmeister, O. K. (2016). The development of assistive dementia technology that accounts for the values of those affected by its use. *Ethics and Information Technology*, 18(3), 185-198.

Burmeister, O. K., Islam, M. Z., Dayhew, M., & Crichton, M. (2015). Enhancing client welfare through better communication of private mental health data between rural service providers. *Australasian Journal of Information Systems*, 19. https://doi.org/10.3127/ajis.v19i0.1206

Burmeister, O. K. & Kreps, D. (2018). Power influences upon technology design for age-related cognitive decline using the VSD framework. *Ethics and Information Technology*, 1-4.

Carlozo, L. (2017). What is blockchain? *Journal of Accountancy*, 224(1), 29.

Cellan-Jones, R. (2014). EU court backs 'right to be forgotten' in Google case. *BBC News* (14 May 2014) online: BBC News Europe< http://www.bbc.com/news/world-europe-27388289.

Dix, A. (1990). Information processing, context and privacy. Paper presented at *INTERACT*.

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, 7(4), 185-200.

Frahat, R. T., Monowar, M. M., & Buhari, S. M. (2019). Secure and Scalable Trust Management Model for IoT P2P Network. Paper presented at the 2019 2nd *International Conference on Computer Applications & Information Security* (ICCAIS).

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 421-471. https://doi.org/10.2307/795891

Hackius, N., Reimers, S., & Kersten, W. (2019). [The Privacy Barrier for Blockchain in Logistics: First Lessons from the Port of Hamburg] *Logistics Management* (pp. 45-61): Springer.

Harris-Brown, E., Luck, N., & Brock, A. (2018). Holochain: scalable agent-centric distributed computing. GitHub. URL: https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf.

Holochain. (2020). *Holochain: think outside the blocks*. Retrieved from https://holochain.org

Holotescu, V. & Vasiu, R. (2020). Challenges and Emerging Solutions for Public Blockchains. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience*, 11(1), 58-83.

Hopwood, D., Bowe, S., Hornby, T., & Wilcox, N. (2016). *Zcash protocol specification*. GitHub: San Francisco, CA, USA.

Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology*, 17(2), 89-101.

Introna, L. (2000). Workplace surveillance, privacy and distributive justice. *SIGCAS Comput. Soc.*, 30, 33-39.

Joshi, J. & Mathew, R. (2018). A Survey on Attacks of Bitcoin. Paper presented at the International conference on *Computer Networks, Big data and IoT*.

Laursen, L. (2015). Google's year of forgetting [News]. *IEEE Spectrum*, 52(5), 16-17.

Metere, R. & Dong, C. (2017). Automated cryptographic analysis of the pedersen commitment scheme. Paper presented at the *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*.

Mittelstadt, B., Fairweather, B., McBride, N., & Shaw, M. (2013). Privacy, risk and personal health monitoring. Paper presented at the *ETHICOMP*, Kolding, Denmark.

Moor, J. (1990). The ethics of privacy protection. Library Trends, 39(1), 69-82.

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., & Narayanan, A. (2018). An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3), 143-163.

Mougayar, W. (2016). *The business blockchain: promise, practice, and application of the next Internet technology*: John Wiley & Sons.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79(1), 119-157.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, US: Stanford Law Books.

Noether, S. & Mackenzie, A. (2016). Ring confidential transactions. *Ledger*, 1, 1-18.

Panichas, G. (2014). An Intrusion Theory of Privacy. *Res Publica*, 20(2), 145-161.

Parent, W. A. (1983). Recent Work on the Concept of Privacy. *American Philosophical Quarterly*, 20(4), 341-355.

Pass, R. (2019). [A tutorial on concurrent zero-knowledge] *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali* (pp. 623-648).

Pass, R., Seeman, L., & Shelat, A. (2017). Analysis of the blockchain protocol in asynchronous networks. Paper presented at the Annual *International Conference on the Theory and Applications of Cryptographic Techniques*.

Posner, R. (1977). The right of privacy. *Ga. L. Rev.*, 12, 393.

Schwartz, P. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review*, 52(6), 1609-1702.

Solove, D. (2002). Conceptualizing Privacy. *California Law Review*, 90(4), 1087-1155.

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477-560.

Stahl, B., Timmermans, J., & Mittelstadt, B. (2016). The Ethics of Computing: A Survey of the Computing-Oriented Literature. *ACM Comput. Surv.*, 48(4). https://doi.org/10.1145/2871196

Teipel, S., Babiloni, C., Hoey, J., Kaye, J., Kirste, T., & Burmeister, O. K. (2016). Information and communication technology solutions for outdoor navigation in dementia. *Alzheimer's & Dementia*, 12(6), 695-707.

Vovchenko, N., Andreeva, A., Orobinskiy, A., & Filippov, Y. (2017). Competitive advantages of financial transactions on the basis of the blockchain technology in digital economy. *European Research Studies*, 20(3B), 193.

Wahlstrom, K. & Fairweather, N. B. (2013). Privacy, the Theory of Communicative Action and Technology. Paper presented at the *ETHICOMP 2013*, Kolding, Denmark.

Wahlstrom, K., Fairweather, N. B., & Ashman, H. (2017). Brain-Computer Interfaces and Privacy: Method and interim findings. Paper presented at the *ETHICOMP 2017*, Turin, Italy.

Wahlstrom, K., Fairweather, N. B., Ashman, H., & Istance, H. (2013). Brain-Computer Interfaces and privacy: clarifying the risks. Paper presented at the Proceedings of the Seventh *Australian Institute of Computer Ethics Conference*.

Wahlstrom, K., Roddick, J. F., Sarre, R., Estivill-Castro, V., & deVries, D. (2006). *On the ethical and legal implications of data mining*. Technical Report SIE-06-001, School of Informatics and Engineering, Flinders University, Adelaide, Australia.

Westin, A. (1967). *Privacy and Freedom*: Atheneum.

Westin, A. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), 431-453.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. Paper presented at the 2017 *IEEE international congress on big data (BigData congress).*

Zyskind, G. & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. Paper presented at the 2015 *IEEE Security and Privacy Workshops*.

doi: https://doi.org/10.3127/ajis.v24i0.2801