The Philosophy of Secrecy: Towards a Historical Analysis of Cryptography, Privacy, and Information Organization

Harry Halpin
Nym Technologies
Place Numa-Droz 2
2000 Neuchâtel, Switzerland
harry@nymtech.net

Abstract

The philosophical definition of privacy is conflated with the secrecy of individual life as guaranteed by the nation-state. We trace the origin of this conception of the nation-state as the guarantor of liberal privacy, and in parallel investigate the claim (by Schmitt) that the historical origin of the modern nation-state is given by the keeping of secrets. From these contradictory claims, we show how the phenomenon of state secrecy and the surveillance of citizens is inherent in the historical development of sovereignty. Finally, we demonstrate the centrality of the history of cryptography to the philosophy of history.

1 Introduction

Within cryptography, the goal of preventing access to information has long lacked philosophical analysis and only recently been subjected to rigorous historical analysis in English (Kahn, 1967).[1] Within its long history, only in the last decades has cryptography been employed to enforce the fraught philosophical concept of privacy. This narrative is held by Whitfield Diffie, who stated that he co-invented public key cryptography to enforce "an individual's privacy as opposed to government secrecy" (Levy, 1994). The prevailing doctrine of privacy holds that it is a relatively new individual right which has only come to the forefront due to its ease of violation by technological developments such as photography and mass media (Westin, 1967). The right to privacy is historically enshrined in legal protections by the state itself rather than technical protections. Thus, due to failures of governments to enforce the right to privacy, cryptography can be used as an privacy-enhancing technology by individuals to enforce control over their own secrets, from any adversary including their own government.

This state of affairs, in which privacy is under threat by private (often corporate actors) and out-of-control governments, could be considered to be a mutation within capitalism (Zuboff, 2018). We would like to turn such a notion on its head. As shown by the history of cryptology, secrecy is constitutive of information organizations of the modern state. This inversion allows us to then consider the increase of government secrecy and the mass surveillance of their own populations to be a historical continuity rather than aberration of the history of the state. It also allows us to reconsider the spread of cryptography from the state to the individual as a shift in the historical landscape of sovereignty, rather than a merely defensive position against some legal lacuna regarding privacy rights and the increasingly digital individual self.

2 The Modern Philosophical Conception of Privacy

The modern concept of privacy is widely considered to have been historically inaugurated in the 19th century by Warren and Brandeis in their *Right to Privacy* (1890). They state that "the protection afforded to thoughts, sentiments, and emotions [...] so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone." Shortly thereafter, the United States assembled a patchwork of common law provisions to protect individual privacy and the United Nations put forward a right to privacy in Article 12 of the Universal Declaration of Human Rights, despite the lack of common constitutional legal precedent: "No one shall be subjected to arbitrary interference with his privacy, family, home or cor-

[1] It should be noted that pre-modern cryptography was systematized in a number of works by German historian Aloys Meister (1902).

respondence, nor to attacks upon his honour and reputation." Europe then followed with a constitutional approach to privacy, reaching its apogee with the Data Protection Regulation that applies principles of consent to an individual's personal data in terms of computer processing.

Despite these seemingly solid legal precedents, considerable philosophical trouble remains even in philosophical legal theory, as there is a long-standing argument over what 'privacy' means (for example, whether privacy constitutes a new right or can be reduced to property rights (Posner, 1977)), with prominent theorists such as Solove claiming that there is no unified philosophical definition (Solove, 2005). At the same time, there has been a revival of interest in using cryptography to preserve the secrecy of personal data and the individual right to privacy (Diffie and Landau, 2010). Although there is newfound philosophical interest in digital privacy in the age of digital data (Véliz, 2021) and the history of privacy as a concept (Vincent, 2016), an historical analysis of the development of privacy and secrecy is missing. This is sorely needed given the well-known history of cryptography in terms of government secrecy (de Leeuw and Bergstra, 2007). Yet this seeming opposition between government secrecy and individual privacy via cryptography may be more dialectical than it first appears.

3 Historical Origins of Privacy

The origin of privacy may very well lie in the murky past of evolution, as even animals such as birds seem to have some natural inclination to privacy in terms of withdrawing into distinct dwellings or territories (Klopfer and Rubenstein, 1977), and the majority of tribes preferred human mating in private dwellings rather than in public (Ford and Beach, 1951). The code of Hammurabi also explicitly creates a law against the intrusion of people into the private dwelling of others (Konvitz, 1966). This division between the public and private as distinct realms becomes explicitly formalized in Aristotle, where the *public* as it relates to decision-making and argument in the polis is given immense value, in contrast to the private realm of domestic dwelling (Reeve, 1998). Public life is given a positive valence with humans being defined as public beings by Aristotle (Reeve, 1998) and the abolition of private life by a communism of women and commodities being put forward as an ideal political organization in Plato's *Republic* (Reeve, 2004).

In contrast, the private is typically given a negative valence as it belongs to the *oikos*, the household and familial life of an individual life which pre-exists, and so Aristotle thought to be inferior to the public life of the polis. The *oikos* is where infamously *idiotes* are constrained, such as women and slaves that are excluded from public life (Reeve, 1998). In this regard, the term 'privacy' and 'deprivation' both descend from *privatus*, being apart from the state and so in a deficient state of being (McStay, 2014). This predominant understanding of privacy as inferior to public life continued in Europe, with the Church in the medieval era functioning as a public administration of spiritual matters, although a private relationship of the clergy and 'holy men' to God retained importance and even became predominant with the rise of Protestantism (Vincent, 2016).

The defense of privacy as a liberal individual virtue then comes from a minoritarian reading of the ancient Greeks, as Socrates admits that his private questioning of virtues would not be possible as part of a public political discussion (West, 1979). Likewise, Aristotle recognizes the virtues of private intellectual pursuits, such as scientific work, as not being easily accomplished as part of public politics (Reeve, 1998). However, this underground tradition of privacy as a realm of virtue was not defended by law in ancient Greece, as is shown by the death of Socrates. The ascendance of the concept of the state as a commonwealth to defend an individual's property rights appears in the 17th century in Locke's *Second Treatise of Government*; privacy is then surprisingly given a positive reading as an individual is guaranteed a private domain – constituted by their property – beyond the possible tyranny of public political life (1689).

Privacy is again described as a virtue in *Utilitarianism* by Mill, which argues that a public government should only interfere in private liberties in order to prevent harm to others, as otherwise the state should guarantee the secrecy of an individual's private life (Mill, 1859). In this vein, Warren and Brandeis' definition of privacy as a legal right to be left alone by (1890) makes sense as a virtue, with the life of ordinary citizens being kept secret by default in contrast to public life. Thus it also follows that the secrecy of private life

is not obtained by prisoners who have violated the implicit legal social contract of liberal societies, although a certain right to mental privacy is obtained even in Bentham's *Panopticon*, namely that "it is to make them not only suspect, but be assured, that whatever they do is known" while leaving "thoughts and fancies to their proper ordinary, the courts above" (Bentham, 1791). With the advent of the Snowden revelations, it appears that the digital panopticon has come to pass.

4 Secrecy as the Foundation of the State

A history of secrecy – including the uses of cryptology – shows the inverse of the liberal hypothesis that the individual's life is the locus of secrecy: secrecy is the province of the state. There are three theories of the birth of the modern nation-state as given by political philosopher Carl Schmitt (Caygill, 2015). In his most well-known theory, the concept of the modern nation-state descends from a secularization of inherently theological concepts (Schmitt, 2005). His second theory is that the emergence of the nation-state was necessary to quell the internecine civil wars of religion at the end of the medieval era (Schmitt, 2008). The last lesser-known theory is that the nation-state descends from the keeping of *arcanum*, or secrets (Schmitt, 1996).

The rise of the literate priestly class that ruled early city-states and empires was at least in part due to their control over information, originating in their knowledge of the valuable relation between agriculture and time (as given by astronomy). This control of information was later extended into records of the storage of food surplus, which later expanded into the storage and transmission of information about resources of all types (Innis, 2022). This information was originally secret, as witnessed by early secret fertility cults and their relationship in Sumer to the anointing of the first kings. Early writing, which was not widely known, could have been considered to be 'secret' knowledge to the vast majority of illiterate people of ancient Mesopotamia. As time progressed in some civilizations such as China, literacy remained the province of a minority in employ of the government, but in other civilizations such as Mesopotamia the spread of literacy caused the invention of what is called 'secrecy statements', where in a text it was explicitly forbidden by the author to share the knowledge in writing with anyone except those with explicit permission given by their position or caste. This literally restricted the information to "one who knows" (*mūdû*), creating a tradition of making a document 'classified' (Mohr, 2022). Thus, we find at the very origins of civilization that writing was an apparatus of information organization on the threshold between the theological and the political insofar as writing was used to maintain the secrets of the emerging state. As more and more people became literate and began to violate these secrecy statements, what appears to be early cryptographic substitution ciphers developed in the historical record of Mesopotamia, protecting both the secrets of religion and the state. As public literacy also increased during the Roman empire, we see the return of substitution ciphers like the Caesar cipher and possibly even more complex ciphers (Reinke, 1962).

In this regard, ancient Greece's notion of the state as an absolutely public space was just as much of a mutation as the development of philosophy as the function of public reason, as witnessed by the persistence of fertility cults based on secret knowledge in ancient Greece and the continued use of ciphers by Greek city-states (Reinke, 1962). The lack of emphasis on privacy as a virtue in individual life in the medieval era was not due to the persistence of the notion of public virtues and private vices from Plato (Reeve, 2004), but was in a sense proportional to the growth of the power of secret knowledge in the Church, which naturally dealt with secrets due to the lack of public literacy in Latin (Innis, 2022). With the decline of empires and the rise of the power of the church came the rise of cryptology being applied to esoteric biblical secrets (Ellison, 2016), and the quest to discover the 'true' (Adamic) names of beings, a tradition transmitted in part from the Arabic medieval world to the early alchemists (Al-Hassan, 2004). However, the relationship between the spread of literacy and the need for cryptography by empires returned to the historical scene with widespread literacy in Arabic in the Middle East and Africa. In parallel to the quest for Biblical knowledge in Europe, the religious impulse to discover hidden knowledge in the Quran re-ignited the field of cryptology, as shown by the work of Al-Farahidi on permutations and the use of frequency analysis of Al-Kindi to break substitution ciphers; this work was politically mobilized by the rise of the

Arabic caliphates, who then weaponized advanced cryptography – as shown by the work of Ibn Adlan on cryptanalysis – to make their own internal communications secret (Schwartz, 2014).

This cryptographic work was then translated and merged with the alchemical tradition, where an *arcanum* of secrets was both simultaneously mystical and practical knowledge (for example, guild secrets as *arcana artis*). This later branched, with the more mystical side of arcana becoming *occultum* (occult) while almost any practical knowledge could become a *secretum*, or secret (including industrial trade secrets such as that of silk production). The use of cryptography became widespread amongst early scientists and intellectuals to defend themselves from the church, as demonstrated by the use of cryptography by Galileo in his trial (Marcus and Findlen, 2019). After the rise of the classical era of Renaissance cryptology given by Cardano, de Vignere, and Della Porta, the art of encoding and deciphering secrets became a profession in and of itself, with professional cryptographers being employed in the diplomacy of Italian city-states in the 15th century (Strasser, 2007). As the civil wars in the rest of Europe came to an end, these techniques were then absorbed into the emerging order of sovereign nation-states of France by cryptographers such as Rossignol and Wallis in England, leading to a new diplomatic order of cryptographers and cryptanalytic 'black chambers' throughout Europe. Although there was some usage of cryptography to conceal scientific discoveries and for other personal purposes (Lochrie, 2011), skilled cryptographers like Wallis were generally put into state service. This increasing monopoly of the nation-state on cryptography became one of the defining aspects of Europe that continued into the era of the world wars and the invention of digital computing, and the invention of modern cryptography by Shannon was originally classified as well (Shannon, 1945). It is only with the invention of public-key cryptography that cryptography became a matter of individual knowledge to the public (Diffie and Hellman, 1976).

5 Contradictions of Secrecy and Privacy

Simmel defines secrecy as the control of information, either by individuals or organizations (ranging from secret societies to the states) (1906). This definition parallels Nissenbaum's definition of privacy as the appropriate flow of information in a social context (2020). A secret has been defined by Bok as the attempt "to block information about it or evidence of it from reaching that person, and to do so intentionally" (Bok, 2011). A secret is a social relation, where information may only be transmitted to its intended reserpine(s). Of course, there is a difference between privacy and secrecy; Bok continues to define privacy as "the condition of being protected from unwanted access" (Bok, 2011), such that secrecy is considered to be non-consensually enforced, while privacy is typically assumed to be consensual. As shown earlier, privacy is ultimately a concept that is indexed to the development of the concept of a sovereign and autonomous human individual whose right to privacy is protected by law and with consent. On the other hand, secrecy is a much wider concept, whose evolution – while grounded also in individuals and networks of trade in Mesopotamia, as per the infamous example of protecting a secret recipe for ceramic glaze (Pearce, 1982) – is ultimately tightly interwoven with the rise of the political theology of state and the formation of hierarchy. As bluntly illustrated by the frontpiece of *Leviathan* by Thomas Hobbes, the state can be considered to be composed of individuals, so conflict is ontologically nullified. Yet this naïve view of the state formation ignores the rise of a ruling class, from kings and scribes to modern-day bureaucrats and cryptographers who are separated from the general population due to their information organization in terms of secrets. Contra Bok, privacy could be simply the application of secrecy to the individual, as her definition does not include the active blocking of access to information, such as via cryptography. Cryptography is simply the technical application of secrecy to information in the presence of adversaries.

It is precisely in this contradiction between state secrecy and individual privacy that the importance of the history of cryptography to the broader philosophy of history is revealed. The state as a purveyor of secrets may guarantee the private lives of citizens from each other, but not from the state itself, which requires transparency from its constituents in direct contradiction to the liberal conception of privacy outlined earlier. Contra Habermas (1985), the state itself is an information organization for the control and transmission of secrets, rather than a publicly transparent space of

democratic decision-making and communication as imagined by the Greeks. This is reflected in how the ancient concept of Greek *polis* arose from the *stasis* – civil war – provoked by persistence of private ties between individuals given by the *oikos*, insofar as the civil war was only resolved as the private lives of individuals were subordinated to the transparent public life of the state (Agamben, 2015). This transparency was viewed as a voluntary virtue in Greece, but has now become an enforced prescription by the state under the rubric of preventing civil war, and is no mere (perhaps temporary) mutation within capitalism (Zuboff, 2018).

This is exemplified by the state simultaneously using cryptography to enforce its own secrets against both other nation-states and its own population. This explains how legislation to increase government transparency is opposed while legislation to increase surveillance powers is supported by the state, and the practice of mass surveillance grows more powerful regardless of the law. In this manner, individuals like Julian Assange who expose state secrets weaken the monopoly of secrecy of the state and so naturally become enemies of the state. On the other hand, the spread of cryptographic techniques such as public-key cryptography outside of the state creates an inevitable schism. Cryptography then both empowers non-state actors (such as multi-national corporations and their digital platforms) to build forms of sovereignty via secrecy at the expense of the nation-state, while individuals can also use cryptographic techniques to preserve their liberal right to privacy technically, rather than only as a legal right that a state may not consent to due to its own security concerns. The public availability of cryptography can then be studied as a historic shift the focus of sovereignty to individuals that wish to escape the transparency that the state enforces on their own population, creating new forms of sovereignty, which leads to the inexorable need for nation-states to break the cryptographic technqiues used by individuals (including those in their own populaton) with the same concern once reserved for competing nation-states.

6 Conclusion

There is perhaps one aspect of being human that serves as the foundation for secrecy: the ultimate interiority of the human mind. With the advent of ubiquitous digital technology, the increased exteriorization of what appeared to be inner cognitive functioning has accelerated, even for the individual (Clark and Chalmers, 1998). This in turn signals the increasing importance of cryptography in terms of maintaining human individual autonomy via secrecy. As the individual becomes more embedded in collective and social technical apparatuses, the concept of privacy may very well be replaced by a broader notion of autonomy. The importance of secrecy as enforced by cryptography will only increase; the information organizations of the future that may very well succeed the Westphalian nation-state will also be based on secret communications between networks of super-empowered individuals, as prefigured in corporations and other social networks. A philosophical analysis should also not only cover the content of communication, but also the structure of the communication network (metadata), as can be defended by technical means like mixnets (Chaum, 1981). A more thorough theoretical meta-analysis is needed with increased reliance on a diversity of archival sources. Note that this treatment has been relatively limited in scope to Europe, and further work should be done in terms of other civilizations such as China and India, with their own histories of privacy, cryptography, and sovereignty. A history of cryptography can be conceived as not only a history of the nation-state, but as the philosophical and political conceptions of sovereignty itself and so an *arcanum* of the philosophy of history.

References

Giorgio Agamben. 2015. *Stasis: civil war as a political paradigm*. Stanford University Press.

Ahmad Al-Hassan. 2004. The Arabic Original of Liber de Compositonae Alchemiae: The epistle of Maryānus, the hermit and philosopher, to Prince Khālid ibn Yazīd. *Arabic sciences and philosophy*, 14(2):213–231.

Jeremy Bentham. 1791. *The Panopticon Writings*. Verso Books (reprinted 2020).

Sissela Bok. 2011. *Secrets: On the ethics of concealment and revelation*. Vintage.

Howard Caygill. 2015. Arcanum: The secret life of state and civil society. *The Public Sphere from Outside the West*, pages 21–40.

David Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90.

Andy Clark and David Chalmers. 1998. The extended mind. *Analysis*, 58(1):7–19.

Karl de Leeuw and Jan Bergstra. 2007. *The History of Information Security: A comprehensive handbook*. Elsevier.

W Diffie and M Hellman. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654.

Whitfield Diffie and Susan Landau. 2010. *Privacy on the line: The politics of wiretapping and encryption*. The MIT Press.

Katherine Ellison. 2016. *A cultural history of early modern English cryptography manuals*. Routledge.

Clellan S Ford and Frank A Beach. 1951. *Patterns of sexual behavior*. Harper Press.

Jürgen Habermas. 1985. *The theory of communicative action: Volume 1: Reason and the rationalization of society*. Beacon Press.

Harold Innis. 2022. *Empire and Communications*. University of Toronto Press.

David Kahn. 1967. *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster.

Peter Klopfer and Daniel Rubenstein. 1977. The concept privacy and its biological basis. *Journal of Social Issues*, 33(3):52–65.

Milton Konvitz. 1966. Privacy and the law: A philosophical prelude. *Law and Contemporary Problems*, 31(2):272–280.

Stephen Levy. 1994. Battle of the Clipper Chip. New York Times.

Karma Lochrie. 2011. *Covert operations: The medieval uses of secrecy*. University of Pennsylvania Press.

John Locke. 1689. *Second Treatise of Government*. Hackett Publishing (reprinted 1980).

Hannah Marcus and Paula Findlen. 2019. Deciphering Galileo: Communication and secrecy before and after the trial. *Renaissance Quarterly*, 72(3):953–995.

Andrew McStay. 2014. *Privacy and Philosophy: New media and affective protocol*. Peter Lang.

Aloys Meister. 1902. *Die Anfänge der modernen diplomatischen Geheimschrift*. Ferdinand Schöningh.

John Stuart Mill. 1859. *On liberty, utilitarianism, and other essays*. Oxford University Press (reprinted 2015).

Sara Mohr. 2022. *Secrecy, Protection, and the Foundations of Knowledge in Ancient Mesopotamia*. Ph.D. thesis, Brown University.

Helen Nissenbaum. 2020. *Privacy in Context: Technology, policy, and the integrity of social life*. Stanford University Press.

Laurie Pearce. 1982. *Cuneiform cryptography: numerical substitutions for syllabic and logographic signs*. Yale University.

Richard Posner. 1977. The right of privacy. *Georgia Law Review*, 12:393.

Charles Reeve. 1998. *Aristote's Politics*. Hackett Publishing.

Charles Reeve. 2004. *Plato: Republic*. Hackett Publishing.

Edgar C Reinke. 1962. Classical cryptography. *The Classical Journal*, 58(3):113–121.

Carl Schmitt. 1996. *Roman Catholicism and Political Form*. Greenwood Publishing Group.

Carl Schmitt. 2005. *Political Theology: Four chapters on the concept of sovereignty*. University of Chicago Press.

Carl Schmitt. 2008. *The Concept of the Political: Expanded edition*. University of Chicago Press.

Kathryn Schwartz. 2014. From Text to Technological Context: Medieval Arabic Cryptology's Relation to Paper, Numbers, and the Post. *Cryptologia*, 38(2):133–146.

Claude Shannon. 1945. A mathematical theory of cryptography. Technical report, Bell Labs.

Georg Simmel. 1906. The sociology of secrecy and of secret societies. *American Journal of Sociology*, 11(4):441–498.

Daniel Solove. 2005. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154:477.

Gerhard Strasser. 2007. The rise of cryptology in the European Renaissance. In *The History of Information Security*, pages 277–325. Elsevier.

Carissa Véliz. 2021. *Privacy is Power*. Melville House.

David Vincent. 2016. *Privacy: A short history*. John Wiley & Sons.

Samuel Warren and Louis Brandeis. 1890. The right to privacy. *Harvard Law Review*, 4(193).

Thomas West. 1979. *Plato's Apology of Socrates: an interpretation, with a new translation*. Cornell University Press.

Alan Westin. 1967. *Privacy and Freedom*. Athenum.

Shoshana Zuboff. 2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.