Ramiro, André; de Queiroz, Ruy J. G. B.

Article

Cypherpunk

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Ramiro, André; de Queiroz, Ruy J. G. B. (2022) : Cypherpunk, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 11, Iss. 2, pp. 1-10, https://doi.org/10.14763/2022.2.1664

This Version is available at:
https://hdl.handle.net/10419/254294

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 11 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Cypherpunk

André Ramiro *Law and Technology Research Institute of Recife (IP.rec)*
andrebramiro@gmail.com
Ruy de Queiroz *Federal University of Pernambuco* ruy@cin.ufpe.br

DOI: https://doi.org/10.14763/2022.2.1664

Published: 26 April 2022
Received: 18 August 2021 **Accepted:** 6 March 2022

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Ramiro, A. & de Queiroz, R. (2022). Cypherpunk. *Internet Policy Review*, *11*(2). https://doi.org/10.14763/2022.2.1664

Keywords: Encryption, Decentralisation, Surveillance, Privacy

Abstract: Cypherpunk refers to social movements, individuals, institutions, technologies, and political actions that, with a decentralised approach, defend, support, offer, code, or rely on strong encryption systems in order to re-shape social, political, or economic asymmetries. Based on a literature review that encompassed the last thirty years, bringing together iconic manifestos, seminal works on Internet social movements, as well as contemporary academic research developments, the entry offers a sedimentation of the significance of cypherpunk phenomena. It argues that "cypherpunk" constitutes a socio technical expression of the promotion of rights through cryptography, meaning that it can be considered to have a broader area of incidence. Therefore, going further in order to give elasticity to the term, the entry covers not only the diversity of political rationale behind the development, promotion and reliance on encryption, but also to classify the variety of expressions of cypherpunk beyond individuals and collectives, but also organisations and technologies that constitute contemporary networks of political participation.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

Definition

Cypherpunk refers to social movements, individuals, institutions, technologies, and political actions that, with a decentralised approach, defend, support, offer, code, or rely on strong encryption systems in order to re-shape social, political, or economic asymmetries.

Origins

In the 1980s, the computer industry was becoming the provider of the main apparatus central to private interconnected management systems and by extension to the United States government's administration. Beyond the optimisation of private and public services, sociopolitical concerns regarding privacy and data protection were already being addressed and gaining space among scholars and activists questioning the necessity of compulsory identification, unnecessary data collection and the formation of data centres, archives and dossiers about individuals (Lyon, 1994; Zuboff, 1988; Burhnham, 1983). The *chilling effect,* which reduces the expression potential of individuals, was potentially growing among civil society (Lyon, 1992).

In parallel, despite the broadening of computer industry and its necessity to provide secure hardware and software that would equip the private sector, the restrictive administrative rules towards domestic use and exportation of encryption (initially listed as a war munition) was imposing an obsolete regulation because the continuing technological development required state-of-the-art security (Diffie & Landau, 2001). This distrust of data collection plus the anachronistic regulation resulted in the advocacy of encrypted technologies becoming to symbolise, at once, a market necessity and a resistance against growing surveillance ecosystems.

The latter was a central concern of a 1985's article, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete,* by computer scientist and cryptographer David Chaum. He dreamed of a transaction model in which, through a strong and reliable encryption system, privacy would be preserved. The premise was that:

> "[c]omputerization is robbing individuals of the ability to monitor and control the ways information about them is used. (...) The foundation is being laid for a dossier society, in which computers could be used to infer individuals' lifestyles, habits, whereabouts, and associations from data collected in ordinary consumer transactions" (Chaum, 1985).

Therefore, for Chaum and for the subsequent cypherpunk movement, the conclusion is that it would be necessary to implement decentralised public-key encryption systems (Diffie & Hellman, 1976; Rivest, Shamir & Adleman, 1978), in order to disrupt this fast-marching problem.

In 1988, influenced by Chaum's ideas and pushing the ideology forward, electronic engineer Timothy May, a then former Intel employee, distributed flyers of a first draft of what would become the *Crypto Anarchist Manifesto*. The manifesto was officially published in 1992 (May, 1992). In that same year, May and Eric Hughes gathered a group of cryptographers, mathematicians, engineers, and hackers for meetings to discuss how encryption communication systems could overcome state surveillance. According to Levy (2001), Jude Milhon, influenced by authors such as Neal Stephenson and William Gibson—known for cyberpunk novels with technological immersive scenarios, and rebellious characters—baptised them "cypherpunks" (a word-play with *cipher*, the central code of an encryption system). The group then adopted the label.

Although Tim May could be considered the most prolific cypherpunk ideologist near the origin of the movement, and close to anarchist beliefs, it is crucial to place him among a varying spectrum of political views within the movement's first founders. Eric Hughes (1993) has published the iconic *A Cypherpunk's Manifesto,* stating that "cypherpunks write code (...) deplore regulations on cryptography" and "are actively engaged in making the networks safer for privacy". The publication was a landmark for also establishing the concept of "cypherpunk" at the time, and it explored the value of privacy within personal data dynamics (for example, anonymization protocols) in expanded connected ecosystems. Then it highlighted the centrality of encryption for the society to achieve a reliable "social contract". John Gilmore (1991), in a paper called "Privacy, Technology, and the Open Society" introduced at the First Conference on Computers, Freedom, and Privacy that year, predicted much of what would be explored by Eric Hughes two years later by combining emerging Internet rights, with a focus on data protection, to the full deployment of strong encryption:

> "What if we could build a society where the information was never collected? (...) That's the kind of society I want to build. I want a guarantee—with physics and mathematics, not with laws—that we can give ourselves things like real privacy of personal communications. Encryption strong enough that even the NSA can't break it" (Gilmore, 1991).

After its inception the term was further crystallised by the creation of the "*Cypherpunk Mailing List",* a forum-like discussion space with nearly a thousand people in the 1990s (Manne, 2011; Greenberg, 2012). The mailing list encompassed a range of people that went from anarcho-capitalists to socialists, leftists to rightists, political scientists and lawyers to developers and cryptographers (Rid, 2016), making it nearly impossible to classify the cypherpunks in one single class, under one stakeholder, or political box. Still, the mailing list gained traction and there was a shared understanding and strategy discussions in opposition to regulatory limitations of domestic use and exportation of encryption products, as well as against major national surveillance programs that would undermine communications secrecy in that decade.

Evolution of the term from a chronological perspective

From a chronological perspective, the wide selection of definitions on the *cypherpunk* spectrum can draw a rich mosaic of interpretations since its baptism back in 1992.

Taking from the first two manifestos mentioned before, Levy (1993; 1994; 2001) offers a continuous documentation of the cypherpunk's first decade. As a description, the author states that they were "cryptographers with an attitude", "a loose confederation of computer hackers, hardware engineers and high-tech rabble-rousers" that "assumed that cryptography is a liberating tool, empowering individuals to protect communications from the Government". Levy's approach offers special attention to their involvement in the 1990's Crypto Wars and their advocacy towards the weakening of government regulations for civilian use of encryption.

In 2006, the term *Cypherpunk* was added to the Oxford English Dictionary as "a person who uses encryption when accessing a computer network in order to ensure privacy, especially from government authorities" (Lexico, 2021). Colin Bennett (2008), in his well known ethnography about narratives and agendas of privacy advocates around the world, credits the cypherpunks as the principal example of the assemblage between *privacy-enhancing technologies* and the notion of anonymous

communications to avoid law enforcement interests. The available definitions gained new dimensions with the advent of WikiLeaks (further discussed below), with Greenberg (2012) and Assange (2012) expanding its social and historical meaning to cover a whistleblowing movement that values secure communication spaces—thus encrypted—in order to report on government and private corporation's abuses.

The notion that cryptography rearranges power is directly shared by the cryptographer Phillip Rogaway, an explorer of the political dimensions of encryption and author of a seminal essay entitled "The Moral Character of Cryptographic Work" (2015). After giving an overview about the connections between technoscientific production and social values, for too long denied by scientists (including cryptographers), Rogaway states that cypherpunks have "long worked the nexus of cryptography and politics". To him, not cryptographers, but cypherpunks are normally the strongest advocates of cryptography: they are "cryptographers with values".

In addition, in a book dedicated to tell the story of cybernetics' main ideas, from Norbert Wiener's first theories of automated control systems to contemporary political techno-dilemmas, Rid (2016) also gives great attention to libertarian movements within, with focus on the cypherpunks. The author relates the movement to the "unshakable cybernetic faith in the machine", that "combined Wiener's hubristic vision of the rise of the machines with [Stewart] Brand's unflinching belief that computers and networked communities would make the world a better place", although adding a crucial key element: cryptography, which would provide the necessary personal empowerment.

Regarding the narratives mobilised by cypherpunks, Hellegren (2016; 2017) introduces the notion of "*crypto-discourses*" to analyse how a rationale was articulated to define "Internet freedom", by having the state as the antagonist actor. The author recalls the concept of *crypto-freedom* from Coleman and Golub (2008), "to refer to a partially fixed construction of meaning that establishes a relationship between encryption and a negative conception of freedom". In other words, "freedom" (or the use of encryption for that matter), to cypherpunks, would necessarily encompass acts to oppose the state's power. It didn't include a public call for an eventual obligation of the state to ensure encryption-derived rights such as privacy or freedom of expression.

Finally, Jarvis (2021) more recently echos that the concept of freedom is "not entirely fixed", arguing that, for example, although Tim May's initial insights were somewhat influential, his conception of freedom did not comprehend the whole

variety of political tendencies within the cypherpunk community, as stated before. They were a highly educated, mostly libertarian community, permeated by *some* aspects of anarchism derived from societal disaffiliation inherited from counterculture circles, influencing generations of digital privacy activists responsible for challenging today's surveillance programs.

The idea of cypherpunk goes beyond individuals

The creation of the mailing list played a central role, and it anticipated the threats to encryption to come. The two main policies were the *Clipper Chip* and "key escrow" proposals by the United States federal government, according to which backdoors would be implemented in encrypted communication systems and a decryption key copy should be escrowed to the government (Kehl; Wilson; Bankston, 2015). The time around these proposals is broadly known as the first *Crypto Wars,* and the proposals have frequently resurfaced in one form or another.

Resisting those policies took a cypherpunk approach by existing as a technosocial *quasi*-organized movement[1] and as an emailing network. But from an institutional perspective, it is possible to credit entities such as the then recently created Electronic Frontier Foundation—co-founded by one of the central figures to the cypherpunk early articulations, John Gilmore—as a cypherpunk organisation, a structured institutional front, with legal powers, to engage in court battles and public advocacy for encryption freedom.

If the cypherpunks' defence of encryption—as a tool to enforce effective secrecy for civil communication and privacy regarding individual's data in transactions—was so far seen as an essential resource to keep away government and private corporations' eyes and ears, an additional layer to its meaning could be perceived within the WikiLeaks movement. The ideology represented by Julian Assange (Assange *et al*. 2012), reaffirms not only the use of strong encryption to protect private communications between two parties, but strengthens the notion of using encrypted communication channels to report on abuse, release secret government information with potential public interest and scandals connected to private corporations. It brings the notion of the protection from identification and the message's content security to whistleblowers. In the words of their model, "privacy for the weak, transparency for the powerful." As a result, WikiLeaks can be considered a *cypherpunk organisation* (Anderson, 2020), adding the element of securely reporting gov-

1. "The only thing they all shared was an understanding of the political significance of cryptography and the willingness to fight for privacy and unfettered freedom in cyberspace", says Manne (2011).

ernment and corporate abuse to the cypherpunk spectrum.

Further, the symbolization of the cypherpunk spectrum is not identified only in individuals, groups, and constituted organisations, but the phenomenon's technical dimension is materialised in the basic element of digital technologies: code. The cypherpunks' defence of encryption was not only a theoretical or law-based activism for human rights, but was coded into software at the very beginning of its activity. In 1991, when *Pretty Good Privacy* (PGP) was published as a strong encryption resource to private communications, it was a fundamental inspiration to the cypherpunk movement. According to its creator, Philip Zimmermann (1999), it was a 1991's surveillance draft bill focusing on backdoors to private communications that made him publish PGP for free in order to popularise the use of strong encryption, so that it would be impossible to revert the situation, for example, by unpublishing the software (Levy, 2001; Greenberg, 2012). It was a strategic intervention in the technological culture, provoking social change. Therefore, PGP can also be qualified as a *cypherpunk technology*. The same interpretation reaches other decentralised technological expressions, such as Bitcoin, conceived in 2008—see Pernice and Scott (2021), bridging early cypherpunk elaborations to current cryptocurrency models—and the The Onion Router (TOR), launched in 2002, and currently maintained by The Tor Project.

It's also worth noting the greater geographical decentralisation of the cypherpunk movement brought by WikiLeaks. If most of the cypherpunk movement in the nineties took place in the United States, there has been a diffusion of whistleblowing movements around the world, coinciding with the advancement and the popularisation of encrypted communication channels. That is reflected in the central role of Julian Assange and figures like Jérémie Zimmerman (Quadrature du Net, from France) and Andy Müller-Maguhn (Chaos Computer Club, from Germany) for the cypherpunk movement. Manne (2011) notes that, for Assange, laws regarding Internet control tended to be harmonised worldwide due to globalisation —meaning a great risk if the laws were inclined to restrict human rights—and, in parallel, to combat this, political actions must be taken on a global scale in order to provoke social change—which happened to be the *modus operandi* of WikiLeaks, helping the spread of the cypherpunk ethos.

Literature has also made it possible to stretch the elasticity of the term "cypherpunk" further by advancing the idea of "cypherpunk" being a characterisation of sociotechnical phenomena beyond individuals. This characterisation brought political dimensions to encryption itself by categorising different types of encryption according to their socio technical purpose. As an illustration, in the taxonomy pro-

posed by Arvind Narayanan (2013), the term "crypto" deserves its own classification according to its purpose. *Crypto for security* would be designed to protect electronic transactions in the context of economic development; "*crypto for privacy*" would be sub-categorized in two others: "*pragmatic crypto*", which aims to "keep the same level of privacy that we had in the analog world", and "*cypherpunk crypto*", that sees in cryptography an engine that inexorably re-shapes economic, social and political power structures.

Finally, the notion that *cypherpunk* can also be instrumental to qualify technologies is sustained by Nabben (2020). In the field of ethnography, she argues, there hasn't been a proper definition to classify *decentralised information infrastructures*, such as blockchain, nowadays best illustrated by cryptocurrency ecosystems. Defined by being *participatory*, *permissionless*, and *encrypted*, these infrastructures could produce digital assets categorised under the heading of *cypherpunk*.

Conclusion

Along with the development of actors and technosocial structures regarding encryption, for the last thirty years the term *cypherpunk* has been used to describe different contexts. Originally used as an adjective to characterise individuals that used encryption as a way to perform social and political change, the term now can be understood as a qualification to individuals, groups, entities and techniques that fulfil its foremost vision: claiming and safeguarding rights and freedoms through encryption, with encryption as the basic and ultimate element. Therefore, it can be asserted that ***cypherpunk*** *refers to social movements, individuals, institutions, technologies, and political actions that, with a decentralised approach, defend, support, offer, code, or rely on strong encryption systems in order to re-shape social, political, or economic asymmetries.*

References

Abelson, H. (2015). *Keys Under doormats: Mandating insecurity by requiring government access to all data and communications* [Report]. Massachusetts Institute of Technology. http://hdl.handle.net/1721.1/97690

Anderson, P. D. (2020). Privacy for the weak, transparency for the powerful: The cypherpunk ethics of Julian Assange. *Ethics and Information Technology*, *23*, 295–308.

Assange, J. (2012). *Cypherpunks: Freedom and the Future of the Internet*. OR Books.

Bennett, C. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. MIT Press.

Burnham, D. (1983). *The Rise of the Computer State: The Threat to Our Freedoms, Our Ethics and Our Democratic Process*. Random House Inc.

Chaum, D. (1985). Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM*, *28*(10). https://dl.acm.org/doi/10.1145/4372.4373

Coleman, G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3). https://doi.org/10.1177/1463499608093814

Diffie, W., & Hellman, M. (1976). New directions on Cryptography. *IEEE Transactions on Information Theory*, *22*(6). https://ee.stanford.edu/~hellman/publications/24.pdf

Diffie, W., & Landau, S. (2001). The export of cryptography in the 20th and the 21st centuries. In *The History of Information Security* (pp. 725–736). Elsevier. https://doi.org/10.1016/B978-0444516008-4/50027-4

Gilmore, J. (1991, March 28). *Privacy, Technology, and the Open Society*. First Conference on Computers, Freedom, and Privacy.

Greenberg, A. (2012). *This Machine Kills Secrets: How WikiLeakers, Cypherpunks and Hacktivists Aim to Free the World's Information*. Dutton.

Hellegren, I. (2016). Deciphering Crypto-Discourse: Articulations of Internet Freedom in Relation to The State. *11th Annual GigaNet Symposium*. http://dx.doi.org/10.2139/ssrn.2909373

Hellegren, Z. I. (2017). A history of crypto-discourse: Encryption as a site of struggles to define internet freedom. *Internet Histories*, *1*(4), 285–311. https://doi.org/10.1080/24701475.2017.1387466

Hughes, E. (1993). *A Cypherpunk's Manifesto*. https://www.activism.net/cypherpunk/manifesto.html

Jarvis, C. (2021). Cypherpunk ideology: Objectives, profiles, and influences. *Internet Histories*. https://doi.org/10.1080/24701475.2021.1935547

Kehl, D., Wilson, A., & Bankson, K. (2015). *Doomed to repeat history? Lesson from the crypto war of the 1990* [Report]. Open Technology Institute, New America. https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/

Levy, S. (1992). Crypto Rebels. *WIRED*. https://www.wired.com/1993/02/crypto-rebels/

Levy, S. (1995). *The Cypherpunks vs. Uncle Sam* (L. Hoffman, Ed.). Institute for Computer and Telecommunications Systems Policy and Department of Electrical Engineering and Computer Science.

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. Penguin Books.

LEXICO. (2006). *Cypherpunk*. LEXICO Powered by Oxford. https://www.lexico.com/definition/cypherpunk

Lyon, D. (1992). The new surveillance: Electronic technologies and the maximum security society. *Crime, Law and Social Change*, *18*(1–2). https://doi.org/10.1007/BF00230629

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press.

Manne, R. (2011). The cypherpunk revolutionary. *The Monthly*. https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary#mtr

May, T. (1992). *The Crypto Anarchist Manifesto*. https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

Nabben, K. (2020). 'An ethnography of decentralised information infrastructure': Adopting cypherpunk nomenclature to categorise the unique attributes of decentralised technologies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3752531

Narayanan, A. (2013). What Happened to the Crypto Dream? *IEEE Security and Privacy Magazine*. https://www.cs.princeton.edu/~arvindn/publications/crypto-dream-part1.pdf

Pernice, I., & Scott, B. (2021). Cryptocurrency. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1561

Rid, T. (2017). *Rise of the Machines: A Cybernetic History*.

Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

Rogaway, P. (2015). *The moral character of cryptographic work* (Report No. 2015/1162). Cryptology ePrint Archive.

Zimmermn, P. (1999). *Why I Wrote PGP*. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

Zubhoff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power*. Basic Books, Inc. Publishers.

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

cnrs centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies