Selected Papers of #AoIR2017:
The 18th Annual Conference of the
Association of Internet Researchers
Tartu, Estonia / 18-21 October 2017

DO CIPHERS HAVE POLITICS?: DISCOURSES OF THE DIGITAL RIGHTS MOVEMENT IN THE CRYPTO WARS 2.0

Sarah Myers West
USC Annenberg School for Communication and Journalism

Encryption is a technical process that has become imbued with tremendous social and political value. It is a critical part of the infrastructure of the Internet, making it possible to safely and securely transmit messages across the network. Encryption technologies are behind every credit card transaction, Bluetooth connection, and mobile phone call made by billions of users worldwide.

Like other forms of infrastructure, encryption could be seen as boring and mundane, "singularly unexciting" (Star, 1999). Despite this, encryption technologies have attracted a tremendous amount of attention in recent years due to debates over whether and under what conditions digital information should be allowed to be encrypted. These debates center on a contestation over two incompatible readings of the sociopolitical value of encryption: on the one hand, historical associations of encryption with the state, and on the other, more contemporary interpretations of encryption as a form of protection against mass surveillance.

This paper seeks to tease out these divergent associations within the Crypto Wars 2.0 – a term intended to evoke a similar policy debate in the 1990s. I attend particularly to the development of a discourse associating encryption with human rights between the 90s and present day, exploring its politics through participant observation at digital rights conferences and interviews with privacy advocates, policy officials engaged in the debate, and technologists working on encryption projects. In so doing, I aim to describe the development of a new political imaginary for encryption in the networked age, one which seeks to redistribute power away from institutions and back to individuals.

Encryption has always been deeply intertwined with power: in the words of one scholar of cryptography, its purpose "is to help those already in power remain in power or those without power attain it" (Ellison, 2008, 284). Over its long history, this power has

Suggested Citation (APA): West, S. M. (2017, October 18-21). *Do Ciphers Have Politics?: Discourses of the Digital Rights Movement in the Crypto Wars 2.0*. Paper presented at AoIR 2017: The 18th Annual Conference of the Association of Internet Researchers. Tartu, Estonia: AoIR. Retrieved from http://spir.aoir.org.

commonly been that of the state; many achievements in cryptography were arrived at under the auspices of military intelligence agencies seeking to translate skills in mathematics and technology into weapons that exploit the weaknesses of adversaries.

As early as the fifth century B.C., Herodotus made claims that the advantage of secret writing helped save Greece from being conquered by the Persian king Xerxes (Singh, 1999). George Washington utilized substitution ciphers and invisible ink to manage his network of spies during the Revolutionary War (Rose, 2006), and the decipherment of the Zimmermann telegram enabled Great Britain to push the United States out of its neutrality and in to World War I (Kahn, 1967).

The invention of public key encryption in the 1970s marked a change in the power dynamics of encryption. This method of encrypting a message without requiring the sender and receiver to know one another was an invention of academic cryptographers, not intelligence agencies. It broke the government monopoly on control of cryptographic technology, opening up the field and facilitating private sector usage of powerful new encryption techniques. It also invigorated a discourse among cryptophiles, who began envisioning new and radical uses for encryption (Levy, 2001).

The work of these cryptophiles, who came to call themselves the cypherpunks, laid important groundwork for the encryption movement of today. In a manifesto, cypherpunk co-founder Timothy C. May reflected: “Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions” (May, 1993). He envisioned the democratic potential of encryption to flatten out power structures, redistributing power away from government institutions and toward individuals.

Similar ideas are expressed in calls for ubiquitous encryption by privacy advocates opposing mass surveillance. For example, in a recent speech Director of the Open Technology Institute Kevin Bankston said encryption “…protects us both from the Maelstrom of an insecure Internet and the 1984 of an unconstrained state that can see into every nook and cranny” (Bankston, 2015). May’s vision can be seen refracted in this discourse; encryption is a tool to bolster the rights of individuals in the face of growing incursions on their privacy by powerful actors – not just intelligence agencies, but also corporations engaged in surveillance capitalism.

Other actors involved in the debate associate encryption with the protection of fundamental human rights. A key text in this discussion is the 2015 report by the United Nations Special Rapporteur on Free Expression, which argued that encryption helps to lower barriers to the free flow of information and creates a zone of privacy necessary to make free expression possible (Kaye, 2015). This dimension of the discourse places less emphasis on the rights of individuals, and more on the capacity of communities to develop the kinds of spaces necessary to for free expression (D. Kaye, Author interview, 2017).

Both of these perspectives are active within the discourse of the digital rights community, and are at work in shaping the implementation of encryption both in law and in code. Cypherpunks both past and present are remarkably cognizant of the idea that “artifacts have politics” (Winner, 1980). Their work is imbued with the sense that the architecture of technologies would lead to certain constructions of power and authority; indeed many of them believed they were participating in a project that would bring forth major social and political change. My analysis thus concludes with the ways in which the construction of law and code by the cypherpunks aims to achieve particular sociopolitical consequences (Winner, 1991).

References

Bankston, K. (2016). A Tale of Two Dystopias: Order and Chaos on the Electronic Frontier. Keynote Address, The Frontiers of Cybersecurity Policy and Law Conference at the Robert S. Strauss Center for International Security and Law, University of Texas at Austin Law School.

Coombs, A. W. M. (1983). The Making of Colossus. *Annals of the History of Computing*, 5(3): 253.

Ellison, K. (2008). Cryptogrammatophoria: The Romance and Novelty of Losing Readers in Code. *Eighteenth Century Fiction*, 20(3): 281-305.

The Guardian. (2016, Aug. 31). Encryption: FBI building fresh case for access to electronic devices. *The Guardian.* https://www.theguardian.com/technology/2016/aug/31/encryption-fbi-building-fresh-case-for-access-to-electronic-devices.

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner.

Kaye, D. (2015). Report on encryption, anonymity, and the human rights framework. Office of the High Commissioner, *United Nations Human Rights Council*. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

Kaye, D. (2017, Feb. 22). Personal interview.

Kehl, D., Wilson, A. and Bankston, K. (2015). Doomed to repeat history?: Lessons from the Crypto Wars of the 1990s. *Open Technology Institute*. https://static.newamerica.org/attachments/3407--125/Lessons%20From%20the%20Crypto%20Wars%20of%20the%201990s.882d6156dc194187a5fa51b14d55234f.pdf

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

May, T. C. (1993). The Crypto-Anarchist Manifesto. *Activism.net*. https://www.activism.net/cypherpunk/crypto-anarchy.html

Rose, A. (2006). *Washington’s Spies: The Story of America’s First Spy Ring*. New York: Bantam Books.

Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Doubleday

Star, Susan Leigh. (1999). The Ethnography of Infrastructure. *The American Behavioral Scientist*, 43(3): 377.

Winner, L. (1980). Do artifacts have politics?. *Daedalus*, 121-136.

Winner, L. (1993). Upon opening the black box and finding it empty: Social constructivism and the philosophy of technology. *Science, Technology, & Human Values*, 18(3), 362-378.