Myers West, Sarah

Article

Cryptographic imaginaries and the networked public

Internet Policy Review

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

Suggested Citation: Myers West, Sarah (2018) : Cryptographic imaginaries and the networked public, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 7, Iss. 2, pp. 1-16, https://doi.org/10.14763/2018.2.792

This Version is available at:
https://hdl.handle.net/10419/214057

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 7 | Issue 2

Cryptographic imaginaries and the networked public

Sarah Myers West
Annenberg School for Communication and Journalism, University of Southern California, Los Angeles, United States of America, sarahmye@usc.edu

Published on 15 May 2018 | DOI: 10.14763/2018.2.792

Abstract: This paper interrogates discourses associated with encryption in contemporary policy debates. It traces through three distinct cryptographic imaginaries – the occult, the state, and democratic values – and how each conceptualises what encryption is, what it does, and what it should do. Situating each imaginary in time through historical research, I consider how they foreground distinct configurations of power and authority. It concludes by describing the development of a new cryptographic imaginary, one which sees encryption as a necessary precondition for the formation of networked publics.

Keywords: Encryption, Privacy, Security, History, Information control

Article information

Received: 19 Dec 2017 **Reviewed:** 26 Mar 2018 **Published:** 15 May 2018

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

URL: http://policyreview.info/articles/analysis/cryptographic-imaginaries-and-networked-public

Citation: Myers West, S. (2018). Cryptographic imaginaries and the networked public. *Internet Policy Review*, *7*(2). DOI: 10.14763/2018.2.792

This paper is part of Networked publics, a special issue of Internet Policy Review *guest-edited by William H. Dutton.*

INTRODUCTION

Scholars in communication and STS have long been concerned with the implications of connective technologies for society, exploring ICTs through the frameworks of the "network society" (Castells, 1996), "culture of connectivity" (van Dijck, 2013), and "network public" (boyd, 2010), among others. In recent years, we have begun to grapple with the runaway effects of connectivity; how networked infrastructures can be used for control (Barzilai-Nahon, 2008; Benkler, 2016), enabling internet companies to accumulate vast amounts of digital data with little transparency (Zuboff, 2015; Pasquale, 2014; Angwin, 2014), and facilitating surveillance by state intelligence agencies (Schneier, 2015; Deibert, 2013) that can be used to manipulate

elections (Kreiss & McGregor, 2017).

This article aims to contribute to this evolving body of work through the study of related policy debates over encryption technologies. In keeping with the theme of this special issue, 'networked publics', I explore the cultural value of cryptography as a potential counterbalance to connectivity. Cryptography enables the transformation of messages or data into code inscrutable to anyone save those with the key to unscramble it. It thus enables us to selectively reveal information to some and not to others; adding asymmetries to the process of communication that imbue messages with new kinds of power relations. Cryptographic systems exert control over access to information through the construction of their infrastructure and design: they push the limits of written communication, experiment with new forms of visual representation of an inscribed meaning, or transform it using mathematics.

But whether and to whom access to the hidden meaning in a text is selectively available is also a social and political question. Recent policy debates over encryption reflect a struggle over the information asymmetries that have arisen in an environment of surveillance capitalism (Zuboff, 2015). Over the last decade, we have undergone a process of deep mediatisation (Couldry & Hepp, 2016), recording the most intimate details of ourselves as we move through time and space. By incorporating technologies to our daily habits, the amount of metadata we produce has bloomed, leading to the production of an infinitesimal number of data traces.

As the Snowden revelations demonstrated, these data traces are not scattered to the wind, ephemeral and fleeting. Rather, they are commoditised, mined for their economic potential and harvested by intelligence agencies in the name of national security (Zuboff, 2015; West, 2017). The work of surveillance scholars situates these transitions in their political and economic context (Lauer, 2017; Schneier, 2014), observing how systems of surveillance lead to new forms of algorithmic control (Pasquale, 2014) and are interwoven with historical patterns of discrimination (Browne, 2015).

The policy debate over encryption centres on questions about whether and under what conditions digital information should be allowed to be obscured by making it indecipherable to anyone who does not have the key to decode it.[1] For privacy advocates, encryption presents an important, if partial, solution to the harms posed by mass surveillance. In the face of growing incursions on our privacy by the state and market and insufficient accountability by regulators, encryption can serve to bolster the rights of individuals. By contrast, law enforcement agencies argue that encryption presents an existential challenge: investigators contend that they are reliant on the ability to collect and use this data in order to track down people engaged in violent extremism, using bulk collection and network analysis to map the communications networks of possible terrorists. They claim that the widespread adoption of encryption could lead to the data traces produced by suspects suddenly "going dark" (Homeland Security Committee, 2016).

These two contrasting perspectives illustrate two distinct conceptualisations of the cultural meaning of encryption. Authorities assert there must be ways of using encryption to protect secrets from adversary nations while granting law enforcement access. Advocates argue this is not mathematically possible without weakening encryption such that it could easily be broken by adversaries. This often resolves into a stalemate due to differing interpretations of what is both technically and mathematically possible and politically desirable.

At its furthest extremes, the encryption debate has displaced the underlying argument over how to synthesise differing incentives between and among state agencies seeking to protect national security and individuals' right to privacy.[2] These arguments verge on treating encryption as a

teleological goal in itself; what Gürses, Kundnani and van Hoboken (2016) refer to as "crypto as a defense mechanism". By reducing the argument to technical solutions, this response fails to account for the political nature of the surveillance problem, undermining its social consequences and ignoring issues of race, gender, and class.

Really, these arguments over encryption are not about the technology itself, but who has access to information and at what scale. The crypto debate centres on the question, what are the 'right' relationships between information and power, and how are these relationships defined? Understanding the politics of encryption requires teasing out these questions in a nuanced way, placing them in dialogue with the broader landscape of social and technological change.

This article contributes to our understanding by tracing several readings of the cultural value of encryption historically through archival research, illustrating how they have evolved over its centuries-long history and surface today in contemporary discourses. I see each of these readings as distinct *cryptographic imaginaries* - conceptualisations about what encryption *is*, what it *does*, and what it *should do*. Following Charles Taylor (2004), I see the cryptographic imaginary as something more than a set of ideas or discourses - it is embodied in both technological architecture and social practice, ways of thinking and ways of being in the world.

My analysis is grounded in a tradition in science and technology studies (STS) that sees technological infrastructures - "those systems without which contemporary societies cannot function" (Edwards, 2003) as both having hard technical materiality and being shaped through social processes. Because these infrastructures are embedded in social arrangements, they can inscribe ethical principles into a system - signaling what is important or of value, whose voice is seen as representative or marginal, or what is seen as non-controversial or mainstream.

Surfacing and making visible the imaginaries we develop around encryption provides an entrypoint to understanding the implications of encryption technologies in a networked society: how ciphers are designed to obscure information to some and not to others, how decisions are made about who can be privy to the secrets they obscure, and who can gain access to the technologies of encryption in the first place. As cryptographer Phil Rogaway writes, "That cryptographic work is deeply tied to politics is a claim so obvious that only a cryptographer could fail to see it" (Rogaway, 2015, p. 3). Understanding *how* it is tied to politics has important normative and legal implications; shaping not only the policy debate, but legal and judicial interpretations of cryptography and the architecture of encryption technologies themselves.

METHODS

The findings in this article are part of a larger multi-sited ethnographic study that traces evolutions in the cultural meaning of encryption in relation to the development of networked infrastructures between the 1960s and present day (Marcus, 1995). The analysis I outline here is largely historical and interpretive in nature, drawing on two years of archival research across collections at Stanford Library, the Computer History Museum, the Smithsonian Museum of Natural History and IBM Research.

In order to make sense of shifts in the cultural meaning of encryption, I first sought to understand cryptography in the context of its broad, historical trajectory. I researched canonical histories of cryptography across a range of disciplines, drawing primarily on computer science, literature, and early modern history, as well as histories that were written for popular audiences.

To select texts for analysis, I conducted general searches related to cryptography and encryption through my university's library, Google Scholar, and at each of the archives listed above. In addition, at each archive I conducted targeted keyword searches of the names of companies active in this space (such as RSA, Public Key Partners, and Netscape) as well as prominent individuals who were engaged in the study of cryptography (such as Martin Hellman, Whitfield Diffie, Ron Rivest, Adi Shamir, Leonard Adleman, and David Chaum), generating further sources of material to study. I coded the archival materials thematically using in vivo coding to identify dominant themes and historical trajectories, then worked within each theme to form a linear narrative that traced the evolution of the thematic material over time.

Though the findings I present largely draw from this historical research, they are also informed by two years of ethnographic field work conducted at conferences where members of the contemporary crypto community gather to discuss their work: these included the Chaos Communication Congress, the Internet Freedom Festival, RightsCon, and the Crypto Summit, among others. In addition to collecting participant observation data, I conducted dozens of interviews with privacy advocates, policy officials, and technologists working on encryption projects. This data was not included in my analysis for the purposes of this project, but was useful for providing context.

Despite this, my findings will inevitably be fragmentary and partial, the product of several limitations: first, there are aspects of cryptography that are notably absent from my analysis, such as its relationship to copyright regimes and incorporation into digital rights management technologies, which I determined to be out of scope for this project. Second, because encryption has historically been seen as a critical national security resource it is subject to the classification regimes of both government and corporate institutions; I was able to access some declassified materials but suspect that there are others that remain classified. Lastly, but importantly, there are gaps in whose voices were represented in the archives: those who spoke were primarily men with high levels of technical expertise and education, even though women and people of colour were actively involved in cryptologic enterprises during World War II.[3] I hope to explore these gaps further in future work.

DEFINITIONS

Most texts on cryptography – its mathematical principles as well as its history – begin with a brief glossary in terms. They generally start with a statement somewhat like the following, from the Oxford English Dictionary: encryption is a "Noun. The process of converting information or data into a code, especially to prevent unauthorised access" (Oxford, 2017). This definition captures a number of different aspects of the concept: encryption as both an object (Noun.) and a process (of converting information or data into code). It is often used, as the definition suggests, "to prevent unauthorised access" – rendering its contents unintelligible to anyone without the key, or the capacity to break the code.

Encryption is also often inscribed into technical artifacts. Here, two new distinctions are drawn around what kind of inscription is involved: *ciphers*, which transpose individual letters in an alphabet, and *codes*, which replace entire plaintext words (Kahn, 1967). Similarly, to *encrypt* or *encipher* something refers to the process of translating a piece of plaintext into a ciphered text, while to *encode* means to translate the meaning of the plaintext into code. When it comes to the process of returning a code/cipher to its original plaintext, the actor's intent comes into play, as well as the environment in which they are acting: if the person has legitimate possession of the

key or the system needed to convert the cryptogram back to its original plaintext, they are *deciphering* or *decoding* the text. If they are a third party adversary – someone without possession of the system or key – they are *cryptanalysing*, or *codebreaking*, the text.

Finally, encryption is increasingly implicated in infrastructure, and the term encryption is often used interchangeably with the systems it is built into. Encryption is a part of contemporary networked infrastructure, inscribed in the structures and technologies of the internet and working invisibly to support the things we do with it (Star & Ruhleder, 1996). Encryption technologies are behind every credit card transaction, Bluetooth connection, and mobile phone call made by billions of people worldwide. They are used during the authentication of connections, protecting the connection between your computer browser and the servers of the websites we navigate to. They protect data at rest, ensuring that private information stored on servers is not easily accessed or changed by third parties. Each of these infrastructures are applications of encryption, constructed by technologists and deployed in particular ways. And thus, there are values and ethical principles inscribed in the depths of the systems that deploy encryption.

CRYPTOGRAPHIC IMAGINARIES

The remainder of this chapter is split into three sections, each describing and analysing a different cryptographic imaginary: the occult, the state, and democratic values. I define the cryptographic imaginary as a concept about what encryption *is*, what it *does*, and what it *should do* that is is embodied in both technological architecture and social practice, ways of thinking about cryptography and putting it to use.

The idea of a cryptographic imaginary owes much to the work of Charles Taylor and his elaboration of the social imaginary. Drawing on his work, I understand a social imaginary to be something broader and more all-encompassing than discourse; it is, as Taylor describes it, "not a set of ideas; rather it is what enables, through making sense of, the practices of a society" (2002, 91). Social imaginaries bridge ideas and practices, they encompass both ways of thinking and ways of being in the world. This is a particularly powerful concept for understanding the ideas that we elaborate around technologies, because it affords a mode of analysis that can include both technical practice and discursive arguments (Kelty, 2005).

In each section that follows, I trace the history of cryptography in association with each imaginary, interrogate the values implicit in them, and explain how these values surface in contemporary policy debates about cryptography.

ENCRYPTION AND THE OCCULT

The first and one of the oldest domains in which cryptography emerged associates the transformation of writing with secrecy, magic, and the occult. This is an association that lives on today as much in the writing of the thrillers of Dan Brown and his 'symbologist' Robert Langdon as in claims by Google CEO Eric Schmidt that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (CNBC, 2009).

Some of the earliest versions of cryptography sought to use encryption as a way of mystifying texts, using obfuscation not so much as a way of masking its meaning from adversaries but

rather as a way to add a layer of symbolic meaning to written words. Early practices include the use of hieroglyphics in Egyptian funerary formulas and rune-writing in Scandinavia and Anglo-Saxon Britain, necromancers in the Roman empire, and the use of codes in religious texts such as the Hebrew substitution cipher Atbash, used throughout the Bible and other Jewish mystic writings to encode the names of important words. The use of codes and ciphers in mystic texts became a subject of fascination for the devoted, who developed a practice of decipherment and interpretation to unlock the deeper meanings embedded in religious texts.

The association of encryption with religious mysticism took on a darker tone by the 16th and 17th centuries, but not necessarily because cryptography was actually used as an occult practice – rather, these associations are more likely tied to the stigmatisation of secrecy by average individuals during this period. The early modern cryptography manual *Steganographia* is a good exemplar. *Steganographia* was published in 1606 by the German cryptographer Trithemius, and for years was held up as an example that tied the emerging discipline of cryptography to the practices of early modern magic (Ellison, 2017, Kahn, 1967). This historical interpretation is understandable – the text of the manuscript makes claims about instructing the reader in the use of spirits to send messages over great distances. But in the 1990s, cryptographers finally deciphered the text of its final volume, revealing these interpretations to be misguided. They found *Steganographia* to be a text that is centrally focused on cryptography, but was disguised to be a book purely focused on magic (Reeds, 1998).

Other early modern cryptographers attempted to disassociate encryption from the occult by aligning it with the emerging disciplines of the liberal arts, repositioning practices once considered to be magic, such as alchemy and astrology, into experimental and scientific practices like chemistry and astronomy (Ellison, 2017, p. 72). Their work would seem, at first, to contrast with the efforts of contemporaries like Robert Boyle, who worked to make the production of knowledge public in order to differentiate matters of fact from matters of belief. Shapin and Shaffer (1985) write of Boyle's efforts to cultivate practices of *experimental witnessing,* observing "Matters of fact were the outcome of the process of having an empirical experience, warranting it to oneself, and assuring others that grounds for their belief were adequate" (Shapin & Shaffer, 1985, p. 25).

But cultural, political, and economic factors during the time period may have indeed required some level of secret communication among participants in the scientific revolution: for example, many of these early scientists faced political dangers from ecclesiastical and civil authorities (Hull, 1985), were incentivised to protect trade secrets (Macrackis, 2010), and retained paraphernalia of secret political and religious orders as a form of bonding within the budding scientific community, such as the adoption of secret names, emblems, and oaths to brotherhood (Eamon, 1985). As such, the popularity of secret communication in the emerging scientific discipline is not necessarily in contradiction with the effort to establish new standards of empiricism grounded in experimental witnessing.

Just as important, the circulation of published texts – encrypted or otherwise – in England during the 17th century was in itself subversive. Manuscripts were often spread by clandestine means in order to evade the eyes of government censors. Secret writing is thus intertwined with the practices of reading and writing, and made urgent by the widespread availability of printed matter through the invention of the printing press (Jagodzinski, 1999). As Ellison writes, cryptography "was as much a global communication system for knowledge sharing as it was also a system for hiding and concealing cultural secrets. It was as much an attempt to standardise communication across nations, ethnicities, and languages as it was a means of discriminating

between audience members and preserving cultural difference" (2017, 17). It was only after the practice of reading and writing became widespread that the concepts of privacy and secrecy finally discarded their occult associations and developed a relatively neutral meaning (Jagodzinski, 1999, p. 24).

The idea that cryptography is an occult practice reflects the idea, as persistent at the time as it is today, that secrecy is a mark of poor moral character. The sociologist Georg Simmel rejected this notion, saying that "secrecy is a universal sociological form, which, as such, has nothing to do with the moral valuations of its contents" (1906, 462). But the notion never fully went away: Facebook CEO Mark Zuckerberg has made statements that suggest that hiding one's identity is a sign of a lack of integrity, reasoning that inhibiting Facebook users' capacity to obscure their identities will lead to more civil discourse.

These views are also reflected in how the use of encryption can become a trigger for surveillance: for example, the use of technologies like the Tor browser is one signal that leads to higher levels of targeting in US intelligence agencies' surveillance systems (Cox, 2014). Such an approach incorporates the common argument that "if you aren't doing anything wrong, you should have nothing to hide" in surveillance architecture, perpetuating the idea that individuals seeking privacy must be undeserving of its protections. However, it neglects to account for the real discrepancies in power between citizens and a surveillance state (Solove, 2007).

These ideas are almost never explicitly contextualised historically or tied to the complex set of factors that related cryptography to occult practices in the early modern era. But the association between cryptography and the occult is powerful: despite the efforts of cryptographers over centuries to establish the practice as a science, it retains the residual mark of these dark associations.

CRYPTOGRAPHY AND THE STATE

Another dominant reading of cryptography centres the art of secret writing as a tool of the state. In this domain, cryptography is used as a strategic advantage over adversaries for states waging war in a geopolitical battlefield. As Lois Potter puts it in her book Secret Rites and Secret Writing: Royalist Literature 1641-1660, "Mystery is an advantage for any party in power, and, since knowledge is power, any party out of power will naturally demand further access to it. At the same time, any party which is denied access to the open expression of its views will express them covertly if it can" (Potter, 1989, p. 209).

The assertion that cryptography has historically been monopolised by state authorities requires some unpacking, however. The contemporary debates over the legal status of encryption reveal contradictions between two overlapping perspectives on the proper role of cryptography within states: cryptography as a tool for national security, and cryptography as a tool for state secrecy. These differing perspectives are increasingly in conflict with one another: whichever of them dominates will have important implications for the configuration of power in the state's orientation toward cryptography.

1. CRYPTOGRAPHY AND NATIONAL SECURITY

Cryptography is a key part of the apparatus of state national security: whoever has access to cryptography has a strategic advantage over adversaries by opening up lines of communication that cannot be intercepted. Thus, many states seek to shore up cryptographic resources by

investing in technologies and in the best minds the discipline has to offer.

Though it is not the only use, the most common way cryptography has been used by states is in the military: for example, Herodotus writes that the use of secret writing saved Greece from being conquered by Xerxes, the Persian king, when an exiled Greek citizen sent a message in code to warn the Spartans of Xerxes' invasion plan (Singh, 1999). It is directly implicated in American involvement in both world wars; the decipherment of the Zimmermann telegram by the British led directly to American involvement in World War I. The failure to piece together deciphered intelligence indicating the attack on Pearl Harbor in time led directly to its entry into World War II (Kahn, 1967). The use of cryptography by military agencies reached a new pinnacle during the wars, employed by nearly all nations engaged in the wars and codified through the formation of new agencies devoted to cryptanalysis and cryptography. Modern histories of World War II attribute the cracking of the Enigma machine as one of the decisive victories that led to the end of the war, while Sweden used cryptography decisively in order to maintain its neutrality (Kahn, 1967).

But cryptography also has an important national security function during peacetime, and is a part of the flowering of modern diplomacy between the 16th and 18th centuries: the principle of secrecy in diplomacy was well-established among European states after the Renaissance (Roberts, 2008), and enacted through the use of encryption of diplomatic communications between ambassadors and their home states. These communications were sometimes intercepted, opened and cryptanalysed by other states on the way, a practice pioneered by the French cryptologist Antoine Rossignol and institutionalised by the formation of Black Chambers by countless other states. The historian David Kahn writes that by the end of the 1500s, most European states kept full-time secretaries who worked to read the ciphered dispatches of foreign diplomats and develop official codes of their own. The sophistication of a state's cryptologic capabilities thus became a strategic advantage not only in war, but in peacetime as well (Kahn, 1967, p. 106-109 & 157-165).

Cryptography in national security is thus about a state's capacity to protect its own communications and to infiltrate the communications of their adversaries. In this sense, it is zero-sum: whoever has the most advanced cryptographic systems has a strategic advantage over others, and can leverage this advantage for both military and diplomatic benefits.

2. CRYPTOGRAPHY AND STATE SECRECY

Cryptography also plays an important domestic function *within* states, by enabling state secrecy. Historically, secrecy by the state was meant to symbolise and safeguard the dignity of rulers and integrity of their functions (Hoffman, 1981), canonised by Tacitus in his history of the Roman empire under the principle of *arcana imperii*, or secrecy for the state (Roberts, 2006). This orientation toward cryptography also seeks to maintain a state monopoly on the practice, but to different ends.

One of the earliest examples of the extensive use of encryption by a government can be observed within the pre-modern bureaucratic systems of the Abbasid caliphate. The Abbasids grew a vibrant commercial industry through the administration of strict laws and low tax rates. In order to maintain this system, administrators relied on the secure communication afforded by encryption to protect their tax records and sensitive affairs of state (Singh, 1999).

More often, secrecy is used to mask corruption and impropriety among sovereigns. For example, King Charles I of England used encryption extensively in his letters, which became the subject of intrigue when they were leaked and published in 1645, revealing among other things his distaste

for Queen Henrietta Marie prior to their marriage. The King made the mistake of keeping unciphered drafts of the letters in his papers, making the decipherment of the remaining texts all the easier once captured. This led to both embarrassment for the already-encumbered British royalist cause and, at the conclusion of the English Civil War, his execution for treason (Potter, 1989).

The embrace of secrecy has harmed states' interests in modern times as well: for decades, the United Kingdom was unable to claim its invention of the first programmable digital computer. Because of the secret nature of the country's advances in cryptography during the war, the UK destroyed all records of its invention of the Colossus, the programmable digital computer used by codebreakers at Bletchley Park to decrypt messages in the days leading up to D-Day. For years, the US-made Electronic Numerical Integrator and Computer (ENIAC) was believed to be the first computer, even though Colossus was operational three years earlier. The machine itself and much of the documentation about it were dismantled or destroyed after the war and kept secret until the 1970s (Singh, 1999, Coombs, 1983).

A series of scandals relating to state secrecy in the 1970s led to an embrace of openness in the United States, though this proved to be short-lived. The Church Committee, formed by the United States Senate found that secrecy in the Executive Branch had led to widespread abuse of powers, including the surveillance of civil rights leaders, attempts at assassination of foreign leaders, and a thirty-year programme by the US National Security Agency (NSA) to obtain copies of telegrams departing from the United States (Schwarz, 2015).

A Task Force on Secrecy concluded in 1970 that "more might be gained than lost" if the US adopted "unilaterally, if necessary - a policy of complete openness in all areas of information" (Moynihan, 61). The findings of the Task Force align with the observations of the sociologist Georg Simmel that "Democracies are bound to regard publicity as the condition desirable in itself. This follows from the fundamental idea that each should be informed about all the relationships and occurrences with which he is concerned, since this is a condition of his doing his part" (Simmel, 1906, p. 469).

The spread of networked technologies has opened up unprecedented opportunities for intelligence agencies, giving them new and significantly expanded capacity to collect data not only on citizens within the country, but from people around the globe. However, unlike during the Cold War, this capacity by no means monopolised by the United States. It has led to a fracturing of the discourse within and between government agencies around the usefulness of encryption: whether or not they see cryptography to be a friend or foe is closely tied to both their incentives and views on the role of information in national security.

For example, over the past forty years, the NSA and its UK counterpart General Communications Headquarters (GCHQ) have sought to limit the use of encryption worldwide: by inserting vulnerabilities into encryption standards (for example, by compromising the random number generator in the encryption standard adopted by the US National Institute of Standards and Technology - NIST), promoting the use of backdoored encryption devices (Levy, 2001), and engaging in legal battles to enable government agencies' access to encryption keys (Harris, 2014).

Some former national security officials have expressed support for adopting a stance that recognises the benefits of encryption, siding with those who see privacy as a necessary part of national security, not an adversary to it (Friedersdorf, 2015). This is a view that the FBI does not share – and neither do the governments of the UK, China, India, Senegal, Egypt, and Pakistan,

all of which have laws that highly control or criminalise public use of encryption projects or otherwise enable law enforcement authorities to compel decryption (Abelson et al., 2015; Levy, 2001). To complicate matters, state secrecy made a forceful return in the years following the War on Terror, resulting in the expansion of systems of classification and adoption of secret tribunals to make critical decisions about surveillance authorisations.

Though the narrative of encryption as a tool of the state continues to be a dominant force in encryption policy, it is increasingly complicated and fraught with inter-agency conflict. Despite these complications, it remains true that when viewed through the lens of state power, encryption becomes part of a battlefield of intelligence in which states seek to exploit the weaknesses of others to their advantage.

ENCRYPTION AND DEMOCRATIC VALUES

The third and final domain that emerged in my research is that of encryption and democratic values. The use of codes and ciphers has a longstanding tradition in the United States reaching back to the Revolutionary War: cryptography and the pseudonymous publication of pamphlets enabled the ideas at the heart of the revolution to circulate and gain popularity on their merit without the risk of immediate suppression by Loyalists (Nagy, 2009).

It also has important roots in the experiences of marginalised communities: for example, individuals fleeing slavery in the American South through the Underground Railroad were assisted by coded messages sewn onto quilts, displayed openly by conductors at waypoints on the trip north. The quilts would indicate safe houses and hiding places, or what kinds of resources were available to passengers in their travels, and were legible only to those with the ability to read the codes hidden within them (Rosenberg, 2003). The use of encryption technologies by communities of colour is a subject particularly deserving of more attention, given the long history of the racialised application of surveillance and its deployment as a means to reify boundaries around communities of colour and enforce their marginality (Browne, 2015).

In his book *Domination and the Arts of Resistance,* James C. Scott writes of practices that enable resistance in the face of the powerful. Scott writes that powerless groups often use what he calls 'hidden transcripts' to enact critiques in the face of the powerful; using disguised forms of expression such as rumors, gossip, folk tales, songs, jokes, and gestures to "insinuate a critique of power while hiding behind anonymity or behind innocuous understandings of their conduct" (Scott, 1990, p. xiii). Here, encryption is a subversive force that balances out asymmetries of power resulting from the increased surveillance capacities of both state and market actors.

By the 1980s and 1990s, amateur cryptographers were experimenting with new ideas about encryption software as an enabler of freedom (Hellegren, 2017). Calling themselves "cypherpunks", this community envisioned a new world in which individuals would gain agency through anonymity. They anticipated the dangers of a fully connected world, and put their hopes in encryption technologies as a means to resist the forces of surveillance. For decades, they worked to build tools compatible with innovations in networked technologies that would allow citizens to disconnect, to protect their privacy, and communicate anonymously. They imagined an internet that put privacy, not connectivity, at its centre, and in so doing sought to use encryption as a form of resistance against institutional power. Their work was not without flaws: many of the tools built by cypherpunks were difficult to use, and they spent relatively little time

trying to encourage mainstream computer users to adopt them. However, the evolution of ideas about cryptography in response to the advancement of networked communications between the 1970s and early 2000s laid important ideological foundations for the work of privacy advocates in the present day.

For example, Chinese netizens have developed elaborate systems of coded internet slang known as *e'gao* that can be used in public on social media platforms to circumvent censorship by authorities. By reappropriating common terms and their homophones to distort or subvert their commonplace meaning, everyday citizens engage in resistance against government oversight. One well-known example is a meme in which netizens adopted the term "river crab" as a stand in for its homophone "harmonious", the signature ideology of then-Chinese president Hu Jintao. As the construction of a "harmonious" society by Hu Jintao came to be accompanied by ever-stricter levels of censorship, netizens began saying that they were "river-crabbed" in place of "harmonised" to signal to others that their words had been censored (Nordin & Richaud, 2014). The adoption of codes in this manner enabled activists to communicate outside the purview of increasingly invasive tactics by the state.

Encryption technologies have also proven useful to whistleblowers, journalists, and human rights defenders. The most famous of these cases is Edward Snowden, who used encrypted tools to protect his communications with the journalist Glenn Greenwald and filmmaker Laura Poitras while blowing the whistle on mass surveillance by the National Security Agency. Encryption enabled Snowden to mask his communications from the NSA long enough to escape to Hong Kong and publish the initial articles from the files he leaked. But, concerningly, the use of encryption by human rights advocates has increasingly served as a justification for oppression by the state: for example, the Zone 9 bloggers, a collective of journalists in Ethiopia who write about political issues and human rights abuses, were arrested and charged, among other things, for using encryption tools to protect their correspondence with sources.

In response to such actions there has been a recent effort to associate encryption with international human rights law. Following the Snowden revelations, the United Nations adopted a resolution on the right to privacy in the digital age. In 2013, then-Special Rapporteur on freedom of expression Frank La Rue drew a connection between the resolution and the use of encryption, writing that "States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption" (Human Rights Council, 2013).

His successor, David Kaye, went on to link encryption explicitly to core values of human rights, arguing that it helps to lower barriers to the free flow of information and creates a zone of privacy necessary to make free expression possible (United Nations, 2015; Kaye, personal communication, 2017). Amnesty International has taken this a step further, declaring that encryption is itself an 'enabler' of human rights: "Encryption is a basic prerequisite for privacy and free speech in the digital age. Banning encryption is like banning envelopes and curtains. It takes away a basic tool for keeping your life private," said Sherif Elsayed-Ali, Amnesty's Deputy Director for Global Issues.

In seeking to associate encryption with human rights, these advocates are establishing that encryption may be a precondition for democratic self-expression and association, by fostering zones of privacy where communities of individuals can join together without fear of surveillance. Cryptography thus can play an important role in creating possibilities for the formation of networked publics. This use of encryption is especially important for marginalised communities

that are disproportionately exposed to the gaze of surveillance by corporations and the state under the conditions of surveillance capitalism (Zuboff, 2015; Browne, 2015; Eubanks, 2017).

CONCLUSION

My analysis treats encryption as not just a technical, but sociocultural process. Though encryption is often treated in an instrumental way - as technologies that can be used for the protection of privacy and security - I argue that cryptography has always been innately intertwined with the interrelationships between written language and culture. This has led to the development of cryptographic imaginaries, concepts about how encryption can be used to configure relationships between information and power that are embodied in technological architectures and social practices.

As I have explored in depth, several different imaginaries centred around encryption have arisen, each of which develops distinct understandings of its purpose and use. The existence of multiple co-existing cryptographic imaginaries is in part why encryption has become the subject of so much controversy: not only do encryption debates centre on different ideas about policy, or about what is mathematically possible, they invoke fundamentally different ideas about the value systems and power discrepancies encryption addresses.

For policymakers attuned to thinking of encryption as a tool for criminals and terrorists, its value as a tool for the protection of privacy may feel trivial. For military and intelligence professionals who see cryptography as a valuable national security resource, it makes sense that it would be regulated in a similar fashion to weaponry. For activists and human rights defenders who rely on cryptography to safely conduct their work, access to cryptography is an enabler of democratic freedoms and necessary precondition for free expression.

Each of these perspectives is informed by particular configurations of access to information, and thus particular ideas about the role of cryptography in a networked society. As I have outlined, cryptography can serve as a corrective for some of the harms networked communications infrastructures make possible - namely, that the technologies that connect and empower us can also be used to surveil and hurt us. Cryptography can create new spaces of possibility for communities to form in an environment of mass surveillance; it can enable those with marginalised identities or marginalised views to create spaces for expression and cultivate relationships with like-minded individuals.

Our ability to communicate with one another across time and space through writing is accompanied by an inevitable need to retain a zone of privacy and disconnection. As historian of cryptography, David Kahn, writes, “as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write” (Kahn, 1967, p. 84).

The imaginaries we develop around the cultural meaning of cryptography will inevitably surface in what kinds of encryption technologies are built, adopted, and implemented in infrastructure. They shape the regulatory policies designed to govern them. Lastly, and perhaps most importantly, they emerge in our social imaginaries about the possibilities of our networked infrastructure.

REFERENCES

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Neumann, P. G. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity, 1*(1), 69–79. doi:10.1093/cybsec/tyv009

Agre, P. E. (1997). *Computation and human experience*. Cambridge, UK: Cambridge University Press.

Amnesty International. (2016). Encryption: A Matter of Human Rights. *Amnesty International*. Retrieved from https://www.amnestyusa.org/reports/encryption-a-matter-of-human-rights/2/

Angwin, J. (2014). *Dragnet Nation: A quest for privacy, security and freedom in a world of relentless surveillance*. New York, NY: Times Books.

Barzilai-Nahon, K. (2008). Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control. *Journal of the American Society for Information Science and Technology, 59*(9), 1493-1512. doi:10.1002/asi.20857

Benkler, Y. (2016). Degrees of Freedom, Dimensions of Power. *Daedalus, 145*(1): 18-32. doi:10.1162/DAED_a_00362 Available at http://www.benkler.org/Degrees_of_Freedom_Dimensions_of_Power_Final.pdf

boyd, d. (2010) Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In Z. Papacharissi (Ed.), *Networked self: Identity, community, and culture on social network sites*. Abingdon, UK: Routledge.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Durham: Duke University.

Calaway, J. C. (2003). *Benjamin Franklin's Female and Male Pseudonyms: Sex, Gender, Culture, and Name Suppression from Boston to Philadelphia and Beyond* (Honors Project). Illinois Wesleyan University. Retrieved from https://digitalcommons.iwu.edu/history_honproj/18/

Castells, M. (1996). *The rise of the network society*. Cambridge, MA.: Blackwell.

Couldry, N. and Hepp, A. (2016). *The Mediated Construction of Reality*. Cambridge, UK: Polity Press.

Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace*. Toronto, CA: McClelland & Stewart.

DeSeriis, M. (2015). *Improper Names: Collective Pseudonyms from the Luddites to Anonymous*. Minneapolis, MN: University of Minnesota Press.

Eamon, W. (1985). From the Secrets of Nature to Public Knowledge: The Origins of the Concept of Openness in Science. *Minerva*, *23*(3), 321-347. doi:10.1007/BF01096442

Edwards, P. (1996). *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press.

Ellison, K. (2017). *A cultural history of early modern English cryptography manuals*.

Abingdon, UK: Routledge, Taylor & Francis Group

Eubanks, V. (2017) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press.

Eve, M. (2016). *Password*. New York, NY: Bloomsbury.

Fagone, J. (2017). *The Woman Who Smashed Codes: A True Story of Love, Spies, and the Unlikely Heroine Who Outwitted America's Enemies*. New York, NY: Dey Street Books.

Friedersdorf, C. (2015, July 30). Former National-Security Officials Now See the Peril of Weakening Encryption. *The Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2015/07/former-national-security-officials-see-the-peril-of-weakening-encryption/399848/

Gill, L. (2018, in press). Law, Metaphor, and the Encrypted Machine. Osgoode Hall Law Journal, 55(2). Working paper version retrieved from https://ssrn.com/abstract=2933269

Gillespie, T. (2006). Engineering a Principle: 'End-to-End' in the Design of the Internet. *Social Studies of Science*, *36*(3), 427-457. doi:10.1177/0306312706056047

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society*, *38*(4), 576-590. doi:10.1177/0163443716643006

Harris, S. (2014). *@WAR: The rise of the military-Internet complex*. Boston, MA: Houghton Mifflin Harcourt.

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. doi:10.1080/24701475.2017.1387466

Homeland Security Committee. (2016, June) Going Dark, Going Forward: A Primer on the Encryption Debate. *House Homeland Security Committee Majority Staff Report*. Retrieved from https://homeland.house.gov/press/house-homeland-security-committee-releases-encryption-report-going-dark-going-forward-primer-encryption-debate/

Huffington Post. (2009). Google CEO On Privacy (VIDEO). *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html

Hull, D. (1985). Openness and Secrecy in Science: Their Origins and Limitations. *Science, Technology & Human Values*, *10*(2): 4-13. doi:10.1177/016224398501000202

Human Rights Council. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. *United Nations General Assembly*.

Jagodzinski, C. (1999). *Privacy and print : Reading and writing in seventeenth-century England*. Charlottesville, VA: University Press of Virginia.

Kahn, D. (1967). *The codebreakers; the story of secret writing*. New York, NY: Macmillan.

Kelty, C. (2005). Geeks, Social Imaginaries, and Recursive Publics. *Cultural Anthropology*, *20*(2): 185-214. doi:10.1525/can.2005.20.2.185

Kreiss, D, and McGregor, S. (2017). Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle. *Political Communication, 35*(2): 155-177. doi:10.1080/10584609.2017.1364814

Lauer, J. (2017). *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*. New York, NY: Columbia University Press.

Levy, S. (2001). *Crypto: How the code rebels beat the government--saving privacy in the digital age*. New York, NY: Viking Books.

Mackrackis, K. (2010). Confessing Secrets: Secret Communication and the Origins of Modern Science. *Intelligence and National Security*, *25*(2). doi:10.1080/02684527.2010.489275

Marcus, G. (1995). Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography. *Annual Review of Anthropology*, *24*, 95-117. doi:10.1146/annurev.an.24.100195.000523

Mundy, L. (2017). *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. New York, NY: Hachette Books

Nagy, J.A. (2010). *Invisible Ink: Spycraft of the American Revolution*. Yardley, PA: Westholme.

Nordin, A. & Richaud, L. (2014). Subverting official language and discourse in China? Type river crab for harmony. *China Information, 28*(1). doi:10.1177/0920203X14524687

Oxford. (2017). Encryption. *Oxford English Dictionary*. Retrieved from https://en.oxforddictionaries.com/definition/encryption

Pasquale, Frank. (2014). *The Black Box Society*. Cambridge, MA: Harvard University Press.

Potter, L. (1989). Secret rites and secret writing: Royalist literature, 1641-1660. Cambridge; New York: Cambridge University Press.

Rogaway, P. (2015). The Moral Character of Cryptographic Work. *IACR Cryptology ePrint Archive*, 1162. Available at https://eprint.iacr.org/2015/1162.pdf

Rosenberg, A. (2003). *Cryptologists: Life Making and Breaking Codes*. New York, NY: Rosen Publishing Group.

Schneier, B. (2015). *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W.W. Norton and Co.

Schwarz Jr., F. (2015). *Democracy in the Dark: The Seduction of Government Secrecy*. New York, NY: The New Press.

Scott, J.C. (1990). *Domination and the Arts of Resistance: Hidden Transcripts*. New Haven, CT: Yale University Press.

Shapin, S. and Schaffer, S. (1985). *Leviathan and the Air-Pump*. Princeton, NJ: Princeton University Press.

Simmel, G. (1906). The Sociology of Secrecy and of Secret Societies. *American Journal of*

Sociology, *11*(4), 441-498. Available at http://www.jstor.org/stable/2762562

Singh, S. (1999). *The code book: The evolution of secrecy from Mary Queen of Scots to quantum cryptography*. New York, NY: Doubleday.

Solove, Daniel J. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review*, *44*(4), 745-772. Available at https://scholarship.law.gwu.edu/faculty_publications/158/

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information systems research, 7*(1), 111-134. doi:10.1287/isre.7.1.111

Star, S.L. (1999). The Ethnography of Infrastructure. *The American Behavioral Scientist, 43*(3): 377. doi:10.1177/00027649921955326

Taylor, C. (2004) *Modern Social Imaginaries*. Durham, NC: Duke University Press.

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

Van Dijck, J. (2013) Facebook and the engineering of connectivity: A multi-layered approach to social media platforms. *Convergence*, *19*(2), 141-155. doi:10.1177/1354856512457548

West, S. M. (2017). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*. doi:10.1177/0007650317718185

Williams, J. (2001). The Invisible Cryptologists: African Americans, WWII to 1956. *Center for Cryptologic History, National Security Agency*. Retrieved from https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/african-americans/

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75-89. doi:10.1057/jit.2015.5

FOOTNOTES

1. Though this is a global debate, taking place in the US, EU, Australia, Brazil, China and elsewhere, my analysis, admittedly, will be most representative of American policy discourses. Additional study of these issues in non-US, and particularly non-Western, contexts, is of great value.

2. The notion that there is a binary opposition between privacy and security is contested, see: Gill, 2018 (in press) and Abelson et al., 2015.

3. See, for example: Mundy, L. (2017). *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. New York: Hachette Books; Fagone, J. (2017). *The Woman Who Smashed Codes: A True Story of Love, Spies, and the Unlikely Heroine Who Outwitted America's Enemies*.New York: Dey Street Books; Williams, J. (2001). *The Invisible Cryptologists: African Americans, WWII to 1956*. Center for Cryptologic History, National Security Agency. Retrieved Mar. 31, 2018 from https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/african-americans/.