TallBear, K. (2013) *Native American DNA: Tribal Belonging and the False Promise of Genetic Science,* Minneapolis, University of Minnesota Press.

Tuck, E. and Yang, K.W. (2012) *Decolonization is Not a Metaphor*, in "Decolonization: Indigeneity, Education & Society", 1(1), pp. 1-40.

* * *

Ksenia Ermoshina, Francesca Musiani
Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties, Manchester, Mattering Press, 2022

Michele Veneziano *University of Bologna*

Concealing for Freedom by Knesia Ermoshina and Francesca Musiani is the first book on encryption primarily grounded in STS. It is a much-needed book, that successfully shows how the STS toolkit can advance a socio-technical understanding of encryption, unfolding several major issues that would otherwise remain unrevealed.

Encryption is certainly among those technologies that are perceived as obscure and abstruse by most of the population. Despite the tendency to classify this technology as something for tech-savvy, activists, and war reporters, in recent years there has been a rise in media interest in the issue. Of course, the Snowden 2013 revelations – with which the whistleblower Edward Snowden leaked the existence of highly classified intelligence-gathering surveillance programs run by the U.S.'s National Security Agency and the U.K.'s Government Communications Headquarters – have been a turning point for the field of encryption that started gaining popularity also beyond the specialized circles, becoming a matter of public concern. Since then, the topic has regularly sparked interest. Recently, for instance, after European Commission's proposal to force tech companies to scan private messages protected by end-to-end encryption in search of child sexual abuse materials, several digital rights activists and watchdog organizations started to speak about the "EU war on encryption". Similar debates occurred also concerning the necessity to have a "backdoor" to open encrypted chats to prevent terrorism. Therefore, the topic is tremendously important not only for the impact it has on the personal freedoms of users and citizens but also on social phenomena that are particularly sensitive to public opinion, such as the cases of terrorism and child abuse.

The book originates from a three-year interdisciplinary research project called *NEXTLEAP*, which ran from 2016 to 2018, with the aim of deploying communication and computation protocols for a secure, trust-worthy, and privacy-respecting Internet that could ensure citizens' fundamental

rights. The Authors had two main aims when writing the book: first, to offer what they call an "analytical portrait" (p. 60) of the state of the art of studies on encryption in the messaging field; second, to conceptualize encryption through STS analytical tools and approaches. Both aims are largely achieved. The analytical portrait is rich and detailed thanks also to the Authors' deep knowledge of the field, constructed in more than three years of multi-sited ethnography encompassing participation, activisms and research in encryption circles, conferences and meeting. The Authors provide a fieldwork-driven explanation of emerging systems and communities of "mundane practices" (p. 39) through analytical thick descriptions. The STS toolkit proved all its potential in this journey. The analytical strategy deployed consists of a mixture of ANT (particularly the notions of "translation" and "enrollment"), controversy mapping of the open debates in the specialists' communities, and a more relational sensitivity inspired by Bowker and Star's (1999) work on classifications and standards. Of course, also more recent notions (such as "data activism" and "data justice") find much space throughout the book.

The book is structured in six chapters, plus an introduction that beyond setting the ground for the following chapters, offers an excellent literature review that ranges from social studies on encryption to media studies, computer science, privacy studies, and internet governance studies. The introduction also summarizes the approaches used, the research design, and the main findings of the work, but despite the appreciable effort of proposing a ready-to-use summary, it would be a mistake not to delve into the chapters. It is indeed through the excellent narrative emerging from the thick descriptions of the case studies that the Authors succeed in raising the most interesting insights, stimulating reflections in the reader, and making the reading intellectually lively.

The first chapter of the book is mostly grounded in user and privacy studies. Here Ermoshina and Musiani propose a relational conceptualization of "risk", arguing that when applied to online privacy and security, the notion is mostly a socially defined concept, that largely depends on the user's social graphs and communicative contexts. In this scenario, theoretical tools such as "threat modelling" and "risk assessment" (largely used by experts) become important operative instruments for activists, journalists, and people interested in encryption because they allow them to read the context and understand, according to their needs, what is the best choice for them.

Chapters 2, 3, and 4 are the real analytical core of the book. They aim at gaining an in-depth understanding of three different end-to-end encrypted mail and messaging applications through three case studies, selected according to their underlying protocol (centralized, federated, and peer-to-peer). Chapter 2 presents the case of Signal, a centralized application, and its homonymous protocol that is considered a best practice in encrypted messaging and has become a trendsetter for other projects in

terms of privacy and security features. According to the Authors, this protocol is a "quasi-standard" or "standard by running code" (p. 96), i.e., "something that works" (p. 61) and is iterated and redeployed by others. Centralization is understood as a "control by design" (p. 91) model – in particular, control over changes in the protocol, to respond quickly to technical challenges in situations of uncertainty. Chapter 3 discusses peer-to-peer, decentralized solutions with a focus on Briar, an open-source app that does not use centralized servers. Here the main challenges of the peer-to-peer architecture are discussed (e.g., adoption barrier and dependency on the number of users; the difficulty of managing users' reputations and identities, the role of trust within the architecture). The Authors offer a portrait also of the users of these technologies, especially activists and journalist living in high-risk environments that see a coherence between their political values, based on horizontality, mutual help, self-governance and participation, and the technical architecture of distributed networks. Chapter 4 concludes the analysis of the architectural models with federated messaging technologies, using Conversations, Matrix.org, and LEAP/Pixelated as main cases. Federations emerge as both an infrastructure configuration and a "social experiment" (p. 149), seeking a compromise between more distributed architectures and a high level of security. The federation allows users to choose between different solutions and alleviates the high degree of personal responsibility held by a centralized service provider. It can, however, present security problems due to the difficulty of auditing all the different implementations of a federated protocol. This chapter concludes with an interesting tentative systematization of the "four Cs of federation" (p. 178) (community, compatibility, customization, care), basically four dimensions of analysis for the study of federated technologies. The four Cs model is not merely a rhetorical tool, it is a valuable contribution that organizes in a useful and empirically grounded way the knowledge on federated encrypted systems beyond descriptive factual knowledge. Unfortunately, not all the chapters are along the same lines, and sometimes they tend to remain a bit over-descriptive. Throughout these three chapters the notion of "concealing for freedom" (p. 89), which corresponds to the title of the book, is fleshed out not as a fixed value, but rather as something performed differently in different situations and defined by the context in which it occurs.

After having analyzed so many technologies and protocols, one question naturally arises: how to make sense of the great variety of encrypted messaging solutions present? Inspired by the work of Bowker & Star (1999), Ermoshina and Musiani try to answer the question in chapter 5, investigating the making of the various versions of the Secure Messaging Scorecard (SMS) of the Electronic Frontier Foundation. The updated versions of the SMS gradually moved from an approach that was centered on the technical features of the tools to one centered on the users and contexts of use. The clas-

sification actively participated in the co-shaping of specific definitions of privacy, security, and encryption, placing users at the center of the classification system and giving them a more active role. According to the Authors, narratives, more than indexes, can help unveil what technological tool is the most appropriate for a specific context thanks to their reflexive power that "inspire reflection on who a person is and what they want to do, who their adversary is, and what they want their communicative act to be" (p. 208).

In the last chapter, the Authors, informed by the findings of their fieldwork, argue that the adoption of encryption in messaging systems is inextricably linked to issues of standardization, the political economy of software development, and technical architecture choices. This allows them to conceptualize encryption as a site of social, political and technical controversy.

The book succeeds in offering a compelling and rigorous overview of encrypted messaging systems and the different stakeholders that populate this field, making them accessible and comprehensible also to non-expert readers. *Concealing for Freedom* advances our knowledge about encryption, revealing political and social dynamics that certainly deserve more attention considering the pervasiveness that these technologies have and their impact in a society where much of the communication takes place through these channels. This valuable contribution fits well within the literatures on Internet governance and technical infrastructure (e.g., DeNardis 2009), from which it is inspired. The book differs from the rest of the recently published social studies on cryptography (DiSalvo 2020; Monsees 2019) because it is the first to extensively use and master with proficiency the STS toolkit to investigate the making of encryption systems. Unfortunately, on several occasions, the Authors present important insights that are not fully developed and that remain underexplored. For instance, the intuition of risk as relational is promising but *de facto* remains poorly conceptualized, and the authors seem to overlay this concept with that of contextuality, reminiscent of Helen Nissenbaum's (2010) work on privacy. The notion of quasi-standard also suffers from the same problem of underconceptualization. What is, at the end of the day, a quasi-standard? A stage before becoming a standard or a new ontological understanding of standards as less "rigid" entities? The answer does not clearly emerge from the pages of the book. Despite the convincing skepticism toward classifications of cryptographic systems, it would have been desirable to develop more of a comparative analytical dimension, which is instead left to the reader. The book lacks a chapter explicitly comparing the findings that the authors were able to observe in their intensive period of fieldwork. The goal of this analysis should not be the mere comparison of technological solutions, in search of the phantom best encryption system, but rather emphasize the different social and political dynamics underlying the making of these technologies. Furthermore, as we discussed at the beginning, governments around the world see the widespread implementation of encryption as a

threat to their ability to access online communications. Without entering regulatory issues about the legitimate reasons that governments might have to obtain the content of encrypted communications while in transit, it would have been interesting to explore how the different actors interviewed by the Authors (software developers, activists, etc.) perceive and interact with governmental actors. However, these weaknesses remain marginal in the book and point to future research paths for the scientific community interested in the study of encrypted messaging systems. The value of the book, in addition to its clarity and analytical rigor, lies precisely in its ability to point to a whole range of new research paths, making it a must-read for those looking for a technically informed understanding of how users, developers, designer and journalists are involved in the making of encrypted communications.

References

Bowker, G.C. and Star, S.L. (1999) *Sorting things out: Classification and its consequences*, MIT Press.

DeNardis, L. (2009) *Protocol Politics: The Globalization of Internet Governance*, MIT Press.

DiSalvo, P. (2020) *Digital Whistleblowing Platforms in Journalism: Encrypting Leaks*, Palgrave Macmillan.

Monsees, L. (2019) *Crypto-Politics: Encryption and Democratic Practices in the Digital Era*, Routledge.

Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press.

* * *