CONCEALING FOR FREEDOM

The Making of Encryption, Secure Messaging and Digital Liberties

KSENIA ERMOSHINA

FRANCESCA MUSIANI

foreword by

LAURA DENARDIS

Dec 2021

PRE-PRINT EDITION

Foreword and Introduction

Mattering Press

MATTERING PRESS

Mattering Press is an academic-led Open Access publisher that operates on a not-for-profit basis as a UK registered charity. It is committed to developing new publishing models that can widen the constituency of academic knowledge and provide authors with significant levels of support and feedback. All books are available to download for free or to purchase as hard copies. More at matteringpress.org.

The Press' work has been supported by: Centre for Invention and Social Process (Goldsmiths, University of London), European Association for the Study of Science and Technology, Hybrid Publishing Lab, infostreams, Institute for Social Futures (Lancaster University), OpenAIRE, Open Humanities Press, and Tetragon, as well as many other institutions and individuals that have supported individual book projects, both financially and in kind.

We are indebted to the ScholarLed community of Open Access, scholar-led publishers for their companionship and extend a special thanks to the Directory of Open Access Books and Project MUSE for cataloguing our titles.

MAKING THIS BOOK

Books contain multitudes. Mattering Press is keen to render more visible the unseen processes that go into the production of books. We would like to thank Joe Deville, who acted as the Press' coordinating editor for this book, the two reviewers Andrew Clement and Maxigas, Steven Lovatt for the copy editing, Jennifer Tomomitsu for the proof reading and work on the book production, Alex Billington and Tetragon for the typesetting, and Will Roscoe, Ed Akerboom, and infostreams for their contributions to the html versions of this book.

COVER

Cover art by Julien McHardy.

First edition published by Mattering Press, Manchester.

ISBN: 978-1-912729-22-7 (ppk)
ISBN: 978-1-912729-23-4 (pdf)
ISBN: 978-1-912729-24-1 (epub)
ISBN: 978-1-912729-25-8 (html)
DOI: doi.org/10.28938/9781912729227

CONTENTS

LIST OF FIGURES

AUTHORS

KSENIA ERMOSHINA and FRANCESCA MUSIANI are tenured researchers at the French National Centre for Scientific Research (CNRS). They are based at the Centre for Internet and Society, which Francesca co-founded and co-directs. From 2016 to 2018, Ksenia and Francesca worked within the H2020 project NEXTLEAP (NEXT-generation techno-social and Legal Encryption, Access and Privacy). Their research explores Internet infrastructures and architectures as tools of governance (and resistance) in today's digital world.

LAURA DENARDIS is a globally recognised Internet governance scholar and Professor in the School of Communication at American University in Washington, DC, where she also serves as Faculty Director of the Internet Governance Lab. With a background in information engineering and a doctorate in science and technology studies, she has published seven books and numerous articles on the political implications of Internet architecture and governance.

FOREWORD

THE POLITICAL LIFE OF ENCRYPTION

Laura DeNardis

WHAT HAPPENS IN CYBERSPACE NO LONGER STAYS IN CYBERSPACE. A ransomware attack on a fuel pipeline company leads to long lines at gas stations. A healthcare system data breach prevents people from receiving medical care. An infiltration into a home video security system leads to egregious violations of personal privacy. Foreign probing of digital voter rolls reduces trust in democracy. And security disruptions to cyber-physical industrial systems are also disruptions of our food supply, livelihoods and ability to function in daily life.

Being 'offline' is no longer a defence against the effects of any of these disruptions. People who have never even been on the Internet can be affected by, for example, a data breach of credit card information at their favourite retail store or be harmed by a security vulnerability in a telemedicine device. The complication of society's digital dependencies, with all of its undoubted upsides, is that the security of everything in life now depends upon strong cybersecurity. Hence, cybersecurity is a great human rights issue of our time. Democracy, financial transactions, consumer safety and the stability of all industrial sectors now depend upon it just as much as personal privacy does.

Strong encryption solves many of these concerns. Yet those who have invented the numerous ingenious encryption protocols over recent decades sometimes express surprise that widely available and strong encryption is not implemented everywhere in digital society. Is this merely because of the cost or processing power required for strong encryption, or something more complex?

Encryption is arguably the most politically charged of all Internet technologies. The ability of governments to apply encryption and break encryption has been at the core of diplomatic strategies, foreign intelligence, law enforcement and national security approaches for decades. The complication is that encryption – and especially encryption strength – is a site of contestation and tension between competing values, even within a single government. National security now requires strong cybersecurity around critical communication and industrial systems, and the digital economy. But at the same time, governments also have an interest in weak encryption for law enforcement and intelligence gathering purposes. Law enforcement personnel sometimes call this the 'going dark' problem, where encrypted messaging and encrypted devices become inaccessible for routine evidence gathering. The intelligence necessary for counter-terrorism similarly depends upon the ability to access encrypted communications.

Societal requirements for strong encryption – for securing financial transactions, defending infrastructure and protecting the right to privacy – are directly opposed to the societal requirement that law enforcement and intelligence agencies need access to encrypted information, or more authoritarian surveillance approaches that monitor and control the lives of citizens. This same tension exists between privacy and the invasive business models that rely upon personal data gathering in exchange for customised online ads. Many of the largest technology companies do not charge users for their services but they rank among the highest revenue generating institutions on the planet by collecting the personal data of users and converting this into revenue.

Responding to these tensions and the dynamic norms around the global intersection of security, privacy and social control, different governments have established diverse regulatory approaches to encryption technologies, ranging from banning some outright, to restricting exports to certain countries, to requiring licenses to use them. Because of the political stakes of encryption, it is not surprising that cryptography has sometimes been regulated under the same statutes as firearms and munitions.

In short, cryptography occupies a powerful place in modern society. It is a highly politicised lever of power balancing trust in the economy and democracy, national security, human safety, individual privacy, and law enforcement and intelligence gathering functions.

Considering the stakes, there has not been sufficient examination of encryption and secure messaging as a central lever of infrastructure politics. *Concealing for Freedom* is a much-needed book that cracks open the black box of encrypted secure messaging and discusses the consequences for freedom and online civil liberties. Secure messaging and tools are not just born when implemented into products or regulated by governments. They are created by design communities. And they are shaped by designers who make technical decisions that consider risk, threat models, business models, sociopolitical context and technical constraints. Decentralised versus centralised? Localisation versus globalisation? Anonymous or pseudonymous approaches? What counts as 'good' or 'desirable' security? The standardisation process itself, and design decisions about arrangements of architecture, are also arrangements of power.

Fundamental human rights such as personal privacy and free speech, and the right to trust in digital infrastructures and economies, are shaped by communication protocols. The tension in protocol design between security and privacy has a long history, but it came to the fore after American government contractor Edward Snowden's disclosures about the massive extent of National Security Agency (NSA) surveillance. Internet protocol designers immediately called for 'hardening the Internet' with more extensive end-to-end encryption. The Internet Engineering Task Force (IETF) published consensus documents suggesting that indiscriminate surveillance of either content or metadata was an assault on individual privacy that should prompt stronger encryption choices that make such surveillance either less possible or more expensive. These designers acknowledged both the importance of individual privacy and also the need to restore trust in the Internet. This wasn't the first-time protocol designers would push back against government surveillance.

The political and social stakes around encryption continue to rise as government and corporate surveillance approaches alike become more sophisticated, but also as new technologies emerge. As the Internet has leapt from two dimensional digital screens to the three-dimensional objects all around us – the Internet of Things – so the consequences for privacy and national security have become starker. There is also well-founded speculation about how rapid advancements in quantum computing power may intersect with encryption technologies, possibly cracking historically entrenched cryptography.

Considering the political pressure and the momentum of invasive and powerful emerging technologies, society may already be at a tipping point. We must design a world in which privacy and security are still possible.

PREFACE

A NOTE FOR READERS

THIS BOOK TELLS STORIES ABOUT ONLINE LIBERTIES SHAPED BY TECHNICAL architectures and infrastructures. It originates from a three-year research project called NEXTLEAP (nextleap.eu, NEXT-generation Techno-Social and Legal Encryption, Access and Privacy, funded by the European Commission in the frame of the H2020 Collective Awareness Platforms (CAPS) programme). The purpose of NEXTLEAP, which ran from 2016 to 2018, was to 'create, validate, and deploy communication and computation protocols that can serve as pillars for a secure, trust-worthy, annotable and privacy-respecting Internet[1] that ensures citizens' fundamental rights'[2]: as such, it was an interdisciplinary project at its core. Its consortium included computer scientists and social scientists working in close dialogue with one another in an attempt to build a protocol that 'actually works'. The project was founded in the immediate aftermath of the Snowden revelations, which made technical work surrounding encryption much more of a political issue than it had been in the past, even the fairly recent past, and showed the extent to which sociopolitical factors are crucial in assessing the worth of specific communication technologies vis-à-vis issues such as privacy protection and surveillance. Our role within the project, in close dialogue with technical partners, was to conduct an extensive sociological investigation of technical development processes and user adoption in the field of encrypted secure messaging.

Reflecting this interdisciplinary background, the book is somewhat of a hybrid object, as the research it is based upon was produced with different (albeit entwined) objectives, including to inform the very practical technical discussions among the project developers, to fuel interdisciplinary work in collaboration with computer scientists and to advance a science and technology studies (STS)- and sociology of innovation-oriented understanding of phenomena such as encryption and distributed architectures. We therefore thought it might be helpful to provide readers with some guidance about how to engage with the book, which might depend on their interests, backgrounds or even reading styles. Moreover, in order for the book to be as accessible as possible, a glossary has been included at the end of the book that provides definitions for the technical terms we use.[3] While some of these terms are especially crucial in the discourses and practices of developers, and as such will (also) be unpacked as the chapters unfold, we believe that a glossary can be useful as a general resource. We also provide a comprehensive list that explains the many abbreviations and acronyms that characterise this field. This is located before the book's Introduction. The book does not have an index, but as an Open Access text, e-book versions are freely available to download, so users can search for particular terms that interest them.

During our fieldwork we had the opportunity to meet and talk with many professionals, ranging from cryptographers to user experience and user interface (UI/UX) designers, trainers and users, who mentioned in our discussions (both recorded and off the record) the protocols and tools we focus on here. Moreover, as we continue to be engaged within the field of cryptographic tools and protocols ourselves, as usability researchers, we have been exposed to many ongoing debates in the community around such tools and protocols, and their implications for the field of encryption in secure messaging. This social science research, deeply embedded among technologists, and ultimately improving technology, is in our view one of the stand-out features of this book.

The book has two distinct but interrelated aims: first, to provide what we call an 'analytical portrait' of the state of the art of the highly complex and technical secure messaging field. While the field is changing rapidly and is becoming more of a matter of interest for the general public, it is in our view important to capture the details of how the different technologies and social practices that compose this field emerged, interact and currently operate. In this sense, one of the book's key contributions is to provide something akin to an analytical history of the present, creating a new record of a phenomenon that, even as it continues to develop, is changing the terrain of digital social life in myriad major ways. To make an analytical portrait, as we understand it, means to retrace the development of an artefact – in particular, moments of crises, debates, controversies – to try and understand the 'life' of a few selected encrypted messaging applications, from their creation to their appropriation and reconfigurations by users, to their becoming, in some instances, a subject of public debate, of governance and of lobbying.

The second, related aim is to conceptualise this phenomenon via tools and approaches that have been developed in the social sciences, with a particular focus on bringing to the field of secure messaging insights from STS. Indeed, encryption, the making of secure messaging tools that adopt it as its core principle, and the co-shaping of particular definitions of digital 'freedom', can be read through the lenses of questions and issues that have long been of concern to STS. These range from the effects of competing imaginaries and visions on the day-to-day enactment of technical innovation, to the performative effects that processes of categorisation and 'sorting things out' have on the structuration of a field. Writing with these issues in mind implies engaging in close dialogue with the established STS literature on socio-technical controversies, infrastructure- and architecture- embedded governance and the political value of 'mundane practices'. While the style of writing used when engaging with these questions may be unfamiliar to those outside the discipline, the intention is to advance the conceptualisation of encryption as an intimately 'socio-technical' phenomenon, a foremost example of why, today, digital communication technologies are controversial and contested, why they are both a target and tool of governance, and why they have assumed a fundamental place in the exercise of authority and power.

The book begins – in the introductory Chapter 0 and Chapter 1 – by introducing how a social science perspective can inform the understanding of very broad technical questions, such as encryption and decentralisation; it then progressively narrows its focus to issues specific to secure communications, such as the relationality of risk and the meaning of elaborating a threat model. In Chapters 2, 3 and 4 the book shifts to provide distinct analytical portraits of the field. It presents several case studies of secure messaging projects, including a real-time history of innovations in the making. The book then gradually shifts back in Chapters 5 and 6 to a more explicitly social science- and STS-informed mode of analysis, by examining issues such as sense-making and categorisation attempts in this field, and the implications of the 'making of' Internet freedoms via secure messaging for Internet governance.

As such, the different chapters in this book may 'matter' in different ways to different readers. Readers expecting higher levels of conceptualisation, drawing from STS traditions and the literature of technology and innovation in society, may be more immediately familiar with Chapters 0, 1 and 5, where notions such as 'translation' in an actor-network theory sense, Bowker and Star's 'sorting things out', as well as more recent STS-inspired notions of data justice and data activism are fundamental tools to analyse the fieldwork. However, these chapters should not be neglected by readers from more technical backgrounds, since they bring to light the relational and highly socially embedded nature of some tools that help users in their great diversity 'make sense' of the tools technologists build.

Admittedly, however, technologists will probably feel more at home in Chapters 2, 3 and 4, which focus more on technical analyses of the case studies and on how the technical architecture of different projects co-shapes development choices and user practices. Nevertheless, we would emphasise again that insights from STS inform these chapters in more ways than may appear at first sight. Indeed, by unveiling phenomena such as informal standardisation processes, controversies around different implementations of a particular protocol and trade-offs between usability and technical efficiency, the concepts and methods of STS are both inextricably entwined in shaping our perspectives and embedded in our writing.

While this book is likely to be of primary interest to the readerships described above, we hope that it may spark interest in wider readerships, including those categories of actors that have been so kind as to participate in our fieldwork – developers, activists, journalists, and, last but not least, users. For these groups of readers, we are hopeful that this book may prompt, or, perhaps more modestly, fuel, a series of ‘taking stock’ discussions on their practices with and around privacy-protecting communication tools. We also hope that regulators may find reasons to take pause and reflect upon our analysis. This is likely to happen most prominently in the concluding chapter, which is not simply the sum of the conclusions arrived at in previous chapters but a substantive discussion of, and overture towards, several pressing Internet governance issues of our time as they relate to the security of communications. This book has the not-so-concealed objective of being useful to these publics, at a time when encryption is as much, or ever more, a pressing societal concern as a technical one.

The field of encrypted messaging does not stand still. As we write this note, in November 2020 and in the context of a pandemic-driven increase in surveillance, we can observe new contributions that explore the links between civil liberties and encryption, such as UNICEF’s working paper on children, encryption and privacy[4], alongside new threats to encryption, such as a resolution proposed by the Council of the European Union that controversially calls for a discussion of how to ‘better balance’ the two principles of ‘security through encryption and security despite encryption’.[5] Such cases provide reminders – and there will certainly be more by the time this book is published – of the need for a technically-informed social and political analysis of what encrypted communications are ‘made of’, and of the definitions of freedom they co-produce. We hope that this book will be a lasting contribution towards this goal, and we look forward to it joining the debate.

NOTES

[1] This introductory note is perhaps the best place to highlight the difference between the ‘Internet’ and the ‘Web’, although the two terms are all too often used interchangeably in day-to-day discourse. The Internet is the global system of interconnected computer networks that use a ‘common language’ – namely the Internet protocol suite – to communicate with one another. The Web, or World Wide Web (WWW), is a particular set of applications that is built on top of the Internet, one of the most widely used by end users (along with, e.g. file sharing and e-mail applications).

[2] http://nextleap.eu.

[3] Every time the first instance of a term included in the glossary occurs, it is highlighted in bold.

[4] https://www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html.

[5] https://techcrunch.com/2020/11/09/whats-all-this-about-europe-wanting-crypto-backdoors.

ACKNOWLEDGMENTS

WHEN FINISHING A BOOK, THE TIME OF ACKNOWLEDGMENTS IS A PLEASURE and, to some extent, a surprise. It is at this moment that authors realise to what extent 'their own' work is actually the product of a collective endeavour – formal and informal interactions, moments of feedback and challenge, asking for help and taking stock, thanking and being grateful. To all the individuals and organisations listed below – and those we may have omitted by mistake – we are, indeed, deeply indebted for making this book what it is.

First of all, a heartfelt thank you to Mattering Press for taking this book project on board at the end of 2018, in a time-sensitive situation, and for following it carefully and benevolently ever since. Mattering is a wonderful experiment in researcher-led-and-owned, open publishing that we feel honoured to be a part of. Francesca had been hoping that a book project suitable for submission to MP would come along since she shared the 'keynote spotlight' with Julien McHardy at the 2014 meeting of the Spanish STS network (redCTS), and first heard about the promising nascent Press. She could not be happier that, seven years later, this 'declaration of intentions' which she made in a corner of her mind has come to fruition.

At Mattering Press, we wish to especially thank Joe Deville for the countless, kind and patient hours of work on both the content and form of our book – despite the multiple disruptions in personal and professional lives that the Covid-19 pandemic has caused since early 2020. Thank you so much, Joe.

We wish to thank the team of the H2020 NEXTLEAP project: Jaya Klara Brekke, George Danezis, Giacomo Gilmozzi, Marios Isaakides, Nadim Kobeissi, Wouter Lueks, Vincent Puig, Carmela Troncoso and all the other colleagues who joined the team for shorter periods of time but whose contributions to the project were crucial for its success. A special thanks to NEXTLEAP coordinator Harry Halpin, who first suggested back in 2014 that we should embark on a project on decentralised architectures together and has been a stimulating colleague and co-author throughout the project. A very special thanks to Holger Krekel, head of Merlinux GmbH and lead developer of Delta Chat; we are grateful for numerous insightful and kind conversations during the project, and beyond, on the informatics and philosophy of federation, and for his support of our work. We remember fondly Bernard Stiegler, who prematurely left us on 5 August 2020. His insights permeate the project and its practical and academic outputs.

We also wish to thank the European Commission for funding the NEXTLEAP project via its innovative programme 'Collective Awareness Platforms for Sustainability and Social Innovation' (CAPS). Year after year, CAPS-funded projects have produced very stimulating work on sustainability and citizenship in the digital age, and we hope that this book is another 'brick in the wall' in this regard. Thank you to Fabrizio Sestini and Loretta Anania, EC Project Officers at DG CONNECT, for their attentive and kind spearheading of the project. We are also grateful to Francesca Bria, Maurizio De Cecco and Stefania Milan, who kindly reviewed our work at different stages.

Our heartfelt thanks also go to Laura DeNardis, who graciously agreed to dedicate some time from her extremely busy schedule as Dean of American University's School of Communication – and as one of the world's foremost Internet governance scholars – to write the preface for the book. Her words mean so much to us, as they position our book as a valuable contribution to the academic enterprise that analyses technical infrastructures and architectures as arrangements of power, and they stress the importance of encryption as a core Internet governance controversy of our times.

As this book was developing, a project of a different kind saw the light – the Centre for Internet and Society of CNRS, which Francesca co-founded, and which has been the 'professional home' for us both since January 2019. Thank you to the colleagues who started the adventure of this new research unit with us, this book would not be the same without our ongoing interactions and conversations: CIS co-founder and director Mélanie Dulong de Rosnay, Olivier Alexandre, Maria Castaldo, Jean-Marc Galan, Axel Meunier, Tommaso Venturini and Céline Vaslin. We also wish to acknowledge the interactions with colleagues of the *Groupement de recherche Internet, IA et Société,* that constitutes a vital dimension of CIS. Let us mention here, in particular, colleagues and friends Séverine Arsène, Anne Bellon, Romain Badouard, Lucien Castex, Marida Di Crosta, Clément Mabi, Cécile Méadel, Julien Rossi, Félix Tréguer, Valérie Schafer and Guillaume Sire. We are also indebted to our former research unit, the Institute for Communication Sciences (ISCC) of CNRS, and its director, Pascal Griset, who for three years provided a comfortable and stimulating working environment for the NEXTLEAP project.

Our ability to continue our work on the NEXTLEAP-born investigation on encrypted secure messaging, and on its outputs including this book, was greatly boosted by obtaining funding for a closely related project, *ResisTIC – The Net Resistants: Critique and Circumvention of Digital Coercion in Russia.* Our thanks go to the French national funding body, the Agence Nationale de la Recherche (that also previously funded Francesca's first substantial research project on decentralised architectures, ADAM, a predecessor to NEXTLEAP). We are also grateful to the ResisTIC team: Olga Bronnikova, Françoise Daucé, Fabrice Demarthon, Valéry Kossov, Benjamin Loveluck, Bella Ostromooukhova, Perrine Poupin and Anna Zaytseva, for the fruitful scientific exchanges and friendly conversations in the frame of the project and its seminars.

Over the years, a number of colleagues worldwide, beyond those already cited above, gave feedback on either the book proposal, on papers that eventually formed the basis of chapters or on draft chapters. Thank you, Sylvain Besençon, Nathalie Casemajor, Andrew Clement, Philip Di Salvo, Maxigas, Liudmila Sivetc, Sophie Toupin. Special acknowledgements go to Angela Sasse and Ruba Abu-Salma from UCL, who initiated us into usable security and kindly agreed to discuss our work at a very early stage.

During the writing of the book, Ksenia spent a year and a half at the Citizen Lab (University of Toronto, Canada) as a postdoctoral researcher, and wishes to thank its director Ronald Deibert as well as Masashi Crete-Nishihata, Jakob Dalek, John Scott-Railton, Bahr Abdul Razzak, Miles Kenyon, Lotus Ruan, Adam Senft and all the team. We both wish to acknowledge the Centre for the Sociology of Innovation of MINES ParisTech, where we conducted our PhD theses in a wonderfully stimulating environment and Francesca still holds an associate researcher appointment. Francesca also wishes to thank the editorial team of the *Internet Policy Review,* as well as the Internet Governance Lab of American University, to which she owes a fruitful collaboration with Laura DeNardis, Derrick Cogburn and Nanette Levinson.

More broadly, our work was enriched by a number of academic communities of which we are members. Our thanks go to the International Conferences on Internet Science (INSCI), the Society for the Social Studies of Science (4S) and the European Association for the Study of Science and Technology (EASST), the Association of Internet Researchers (AoIR), the Global Internet Governance Academic Network (GigaNet), The Center for Science and Technology Studies of the European University at Saint-Petersburg, and last but not least, the International Association for Media and Communication Research (IAMCR). Within IAMCR, we wish to acknowledge our joint work with Aphra Kerr, Julia Pohle, Jeremy Shtern and Weiyu Zhang, who co-chair(ed) with Francesca the Communication Policy and Technology Section, and Sylvia Blake, Sibo Chen and Steph Hill, who co-chair(ed) with Ksenia the Emerging Scholars Network.

We write about technical issues that are deeply political, and we hope that our work can be useful to policy. In this regard, being able to interact closely with institutions and NGOs is invaluable. Francesca wishes to thank the French Parliament's Commission for Rights and Liberties in the Digital Age, the CSAlab and the Internet Society France for having engaged with the project and for involving her in their multi-stakeholder reflections on how to make the Internet more open, transparent and usable.

Last but not least, we wish to thank all the activist tech communities that have trusted us, assented to talk to us and assisted in arranging interviews with the most marginalised, at-risk user groups. A very special thanks goes to the Digital Security Lab Ukraine (namely Mykola Kostynyan, Vadym Hudyma, Iryna Chulivska, Maksim Lunochkin and others), Syster Servers collective, Campi Aperti project, Autistici, Riseup, Tails and Espiv. Very warm thanks to dkg, Samba, Vassilis and Spider Alex.

We could not finish these acknowledgments before thanking with all our hearts our families, for their love and support through thick and thin (as the first year of the Covid-19 pandemic concludes, this sentence stands for a whole lot of nuances). Chiara, Jean-Marc, Brune, Loïse, Marco, Patrizia, Carlo, Elena, Oksana, Sasha, Svetlana, Lerie and Timofey: this book is for you.

LIST OF ABBREVIATIONS AND ACRONYMS

A separate glossary of technical definitions is also included at the end of the book.

CAPS	Collective Awareness Platforms
CEO	Chief Executive Officer
CIA	Central Intelligence Agency (United States of America)
CNNum	Conseil national du numérique (French Digital Council)
CTO	Chief Technology Officer
DNS	Domain Name System
DRM	Digital Rights Management
e2e	End-to-end
ECMA	European Computer Manufacturers Association
EDRi	European Digital Rights (organisation)
EFF	Electronic Frontier Foundation
ENISA	European Union Agency for Cybersecurity (maintained original acronym)
ETSI	European Telecommunications Standards Institute
EU	European Union
FBI	Federal Bureau of Investigation (United States of America)
FOSS or F/OSS	Free and Open-Source Software
FSB	Federal Security Service (Russian Federation)
GIF	Graphics Interchange Format
GitHub and GitLab	Platforms for collaboration between developers
GAIM (now Pidgin)	F/OSS Instant Messaging client
GCM	Google Cloud Messaging
GDPR	General Data Protection Regulation
GNU/Linux	Free software operating system

GPG (GnuPG) GNU	Privacy Guard (free-software replacement for PGP)
GPL	General Public License
HADOPI	Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet
HTML	HyperText Markup Language
I2P	Invisible Internet Project
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	information and Communication Technologies
ID	Identifier
IETF	Internet Engineering Task Force
IG	Internet Governance
IM	Instant Messaging
IMAP	Internet Message Access Protocol
iOS	Mobile operating system developed by Apple, Inc.
IP	Internet Protocol
IRC	Internet Relay Chat
IRL	In Real Life
IRTF	Internet Research Task Force
ISO	International Standardization Organization
ISP	Internet Service Provider
ITU	International Telecommunications Union
LEAP	Encryption access project
MENA	Middle East and North Africa (region)
MIT	Massachusetts Institute of Technology
MTS	Telephone company, Russian Federation
MUAs	Mail User Agents
NEXTLEAP	NEXT-generation Techno-Social and Legal Encryption, Access and Privacy (H2020 project)
NIST	National Institute of Standards and Technology (United States of America)
NGO	Non-Governmental Organisation
NSA	National Security Agency (United States of America)

OMEMO	Multi-End Message and Object Encryption (recursive acronym)
OpenPGP	Open implementation of PGP
Opsec	Operational Security
OTR	Off-the-Record Messaging (see Glossary)
OWS	Open Whisper Systems
PGP	Pretty Good Privacy (see Glossary)
p2p	Peer-to-peer (system; see Glossary)
PRISM	Code name for NSA surveillance program begun in 2007
QR-code	Quick Response code
RfC	Request for Comments (IETF)
RightsCon	Summit on Human Rights in the digital age
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SD	Secure Digital
S/MIME	Secure/Multipurpose Internet Mail Extensions (cryptography norm)
SMS	Secure Messaging Scorecard
SMTP	Simple Mail Transfer Protocol
SNI	Server Name Indication
STS	Science and Technology Studies
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
Tor or TOR	The Onion Router
UC	University of California
UDHR	Universal Declaration of Human Rights
UI/UX	User Experience and User Interface
UN	United Nations
UNICEF	United Nations International Children's Emergency Fund
USA	United States of America
USB	Universal Serial Bus (industry standard)
VPN	Virtual Private Network
W3C	World Wide Web Consortium
XMPP	Extensible Message and Presence Protocol
XML	Extensible Markup Language

0

INTRODUCTION

> (F)or a time, I operated part of the US National Security Agency's global system of mass surveillance. In June 2013 I worked with journalists to reveal that system to a scandalised world. Without encryption I could not have written the story of how it all happened […] and got the manuscript safely across borders that I myself can't cross (Snowden 2019a).

THUS WROTE EDWARD SNOWDEN, THE FORMER NSA CONTRACTOR TURNED into the world's most famous whistleblower for digital liberties, on 15 October 2019, shortly after the damning history of his revelations, and the process that led to them, was published under the title *Permanent Record* (Snowden 2019a, 2019b). According to Snowden, the current debates around encryption have fundamental implications for our individual liberties and collective presence on the Internet and attempts to undermine encryption amount to no less than making Internet users 'vulnerable by design'. Encryption has become one of the core battlegrounds of Internet governance.

Indeed, as can hardly be disputed anymore, Snowden's 2013 revelations have been a landmark event in the development of the field of secure communications. Encryption of communications on a large scale and in a usable manner has become a matter of public concern, with a new cryptographic imaginary taking hold, one which sees encryption as a necessary precondition for the formation of networked publics (Myers West 2018). Alongside turning encryption into a fully-fledged political issue, the Snowden revelations catalysed longstanding debates within the field of secure messaging **protocols**. The cryptography community (in particular, academic and free software collectives) renewed their efforts to create next-generation secure messaging protocols in order to overcome the limits of existing protocols, such as **PGP** (Pretty Good Privacy) and **OTR** (Off-the-Record Messaging). Protocols are a vital part of the Internet's functioning, providing its conceptual models as well as the set of specifications that explain how data should be regrouped into packets, addressed, transmitted, routed and received; as Laura DeNardis made clear in *Protocol Politics*, the selection and adoption of particular protocols carries important political and economic implications, as well as technical ones (DeNardis 2009).

With recent events such as the introduction of **end-to-end encryption** in WhatsApp, the most popular instant messaging platform, billions of users started protecting their communications by default and on an everyday basis, often without realising it. While the mantra 'I have nothing to hide' is still widespread among Internet users, interest in ways to secure and preserve online communications with means such as encryption is increasing, and this has important socio-technical consequences. While these consequences apply particularly to those whose lives depend on an accurate appreciation of the risks related to their own profession or political context, they are also ever more relevant to the 'ordinary citizen'.

In response to the increasingly widespread understanding of security in online communications as an important social and political issue, as well as a technical one, encrypted secure messaging is a vibrant field in the making. Developers remain in flux about how to implement security and privacy properties – despite a number of novel projects seeing the light – while users have not yet converged on a single application. For example, there is still debate about cryptographic properties such as **forward and future secrecy**, **group messaging** and **non-repudiation**. Furthermore, there is no clear standard to adopt for these properties. In terms of privacy, work is still immature; even the most popular secure messaging applications, such as Signal, expose users' metadata via the requirement to associate users with their phone number or, in the case of Wire, leak **social graphs** via a centralised contact book.

For all these reasons, next-generation secure messaging appears unstandardised and fragmented, leading to a state where secure messaging users exist in dozens of 'silos', unable to inter-operate (Sparrow and Halpin 2015). The 'silo effect' is considered among the most important obstacles to the adoption of secure messaging apps:

> The common trend of creating new secure communication tools and assessing the usability of these tools is a significant obstacle to adoption due to creating fragmented user bases. Also, to reach their communication partners, participants needed to use tools that are interoperable (Abu-Salma et al. 2017a: 137).

This is in stark contrast to the model used for email, where any email service can openly communicate with another in a federated fashion, agreeing upon collective standards of operation. Thus, developers of modern secure messaging protocols are facing a number of trade-offs between various design issues, including security and privacy properties, the introduction of group support features, the degree of decentralisation of the application, standardisation attempts and choices related to the licenses under which they release their software. In the meantime, vibrant discussions are happening around adapting open federated protocols (e.g. XMPP) to integrate the most recent security features.[1] New initiatives, based on decentralised, federated or **peer-to-peer** protocols are emerging, yet still suffer from a number of limitations related to usability and scalability.

All these dynamics are relevant to this book's examination of developers' actions and their interactions with other stakeholders (users, security trainers, standardising bodies and funding organisations, for instance) and with the technical artefacts they develop, with a core common objective of creating tools that 'conceal for freedom' while differing in their intended technical architectures, their targeted user publics and their underlying values and business models.

As next-generation encryption is shaping the ways in which we can securely communicate, exchange and store content on the Internet, it is important to unveil the very recent, and sometimes less recent history of these protocols and their key applications, to understand how the opportunities and constraints they provide to Internet users came about, and how both developer communities and institutions are working towards making them available for the largest possible audience. Efforts towards this goal are built upon interwoven stories of technical development, of architectural choices, of community-building and of Internet governance and politics. This book is about these stories – exploring the *experience* of encryption in the variety of secure messaging protocols and tools existing today, and the implications of these endeavours for the '*making of*' civil liberties on the Internet.

This book intends to provide two main empirical and theoretical contributions: firstly, it seeks to enrich a social sciences-informed understanding of encryption, including examining how its different solutions are created, developed, enacted and governed, and what this diverse experience of encryption, operating across many different sites, means for online civil liberties; secondly, it wishes to contribute to the understanding of the social and political implications of particular design choices when it comes to the technical architecture of digital networks, in particular their degree of (de-)centralisation.[2]

The first part of this introduction will discuss both of these perspectives. A second part will introduce our case studies, our methodology and approach to our fieldwork. In its final section, in order to facilitate navigation through the following chapters, we situate our case studies in a genealogy of the fundamental protocols in the encrypted messaging field, and we introduce relevant concepts and definitions that will be used in the following chapters, such as end-to-end encryption, centralisation, federation and peer-to-peer/decentralisation.

FOR A SOCIAL SCIENCES PERSPECTIVE ON ENCRYPTION

For quite a long time, 'encryption' as a research subject has mostly been the prerogative of computer scientists, with more 'social' issues concerning it often being confined to debates about usable security (i.e. discussions taking place within the computer scientist community, and based on survey-type studies that aim to find ways of making encrypted tools easier to use). As, since the Snowden revelations, encrypted communications and the goals of privacy and security they seek to enhance are becoming a matter of widespread public debate, it is important that the social sciences take up the challenge of investigating in depth how encrypted messaging tools are conceived and developed, how they are taken up by different user profiles – sometimes in unintended or unforeseen ways – how they inspire and are inspired by different imaginaries, and how they eventually become the target of governance. With this volume, and the three-year investigation it is based upon, we seek to contribute what is, to our knowledge, the first book-length endeavour focused on this subject that is grounded primarily in science and technology studies (STS) and more specifically in the sociology of innovation processes and technical development. First and foremost, our work exists in dialogue with contributions that have recently sought to apply some central concepts in the social sciences, in particular STS, to the study of encryption.

Encryption is a matter of competing imaginaries and of the visions, designs and implementations they co-shape, as Sarah Myers West has recently argued (2018). People think about encryption through cyphers (that transpose letters of an alphabet), and through codes (that replace words) in different social, cultural and political contexts. As Myers West notes, encryption has built its different meanings in the realm of national security and secrecy and in that of democratic systems, in each of which it enables private communication and makes it possible to avoid surveillance and potential social or political sanctions. Myers West's STS-driven investigation into encryption imaginaries is especially resonant with our research, as it illustrates how similar technologies may acquire different meanings and roles in different cultural settings. A particularly important insight is that these technologies should be understood not only in a technical sense but in the specific social, cultural and political contexts in which they are used. Myers West's conclusions are important to emphasise, as this book will provide numerous examples of how technologies (and technologists) do not determine universal solutions when it comes to the role and impact of encryption, with sociocultural contexts of use being paramount. The historical dimension of these sociocultural contexts and their evolution over time should also be taken into account, as Isadora Hellegren points out in her work – grounded in both discourse theory and an STS sensibility – that sees discourse as a contextual, structuring and performative process of meaning-making (Hellegren 2017). The multifaceted meaning of encryption evolves not only across communities of developers and users, but also across time, and understanding how various actors have constructed specific understandings of freedom with regard to technologies like encryption is significant to Internet historians, hackers, programmers and policymakers, as all of these actors are involved in constructing the form, function and meaning of Internet freedom, in particular when it comes to its relation to the state.

Encryption, and the debates around it, are the result of multiple public spheres and expert circles, embedded in broader Internet-and-society questions such as the control of networked media, surveillance and the protection of personal data. Linda Monsees' recent *Crypto-Politics* (2019) is an important contribution to the study of these aspects and more broadly to the development of a social sciences perspective on encryption, even if her primary focus is not the *making* of encryption for a specific use, but rather discourses on encryption as a whole as they unfold in traditional and less traditional political arenas. Monsees uses discourse analysis methods to examine post-Snowden debates related to encryption in both the United States and Germany and describes the landscape of media and specialist discussions as trying to make sense of today's 'diffuse security' – a context where 'security practices disperse multiple insecurities and threat images' (Monsees 2019: 5). Monsees develops the notion of 'publicness' to convey the idea that political controversies on encryption are often located outside established political institutions (although those that unfold in more traditional political arenas should not be neglected). In a way reminiscent of previous work on the performative role of controversies revolving around complex and open-ended sociotechnical phenomena, she concludes, echoing Hellegren, that 'encryption controversies entail specific ideas relating not only to what 'security' means but also how these conceptions rely on specific ideas about citizenship, statehood and privacy' (Monsees 2019: 10).

Beyond the dialogue with this nascent social science scholarship on encryption, our work further seeks to build on, and contribute to, the research of several scholars at the crossroads of media studies, sociology of technology and computer science. They have brought their conceptual and methodological lenses to the study of networked communication technologies and their implications for privacy, security and Internet governance.

The technical development of applications and protocols, and the set of choices involved in this development, critically contributes to making sense of what digital freedoms are, how they should be preserved and who are their adversaries. Anthropologist Gabriella Coleman has paved the way for scholars seeking to explore these questions. In particular, she has examined the role of hacker culture,[3] exploring what hackers mean by freedom and how they enact it as a form of self-determination that considers unrestricted access to knowledge a necessary precondition for the evolution of their 'technical art' (Coleman 2005). Furthermore, Coleman's work is of particular relevance for a social sciences-based study of encryption. Together with Alex Golub, Coleman has defined 'crypto-freedom' as a particular form of hacker practice, grounded in an understanding of freedom that positions the state as the main adversary in the battle for online privacy. This practice is derived from the particular historical and cultural context of liberalism in the United States and grounded in the belief that this freedom should primarily be preserved and fostered on the Internet through the development and use of encryption technology (Coleman and Golub 2008).

Since the Snowden revelations, several authors have tackled the question of what it means to be online as an individual, a citizen and a consumer in a world that is now broadly aware of the extent to which we are being surveilled. Within this realm, they have focused on the issue of the role played by the technical development of the architectures and infrastructures of online communication.

As explored by the work of Stefania Milan and colleagues (e.g. Milan and van der Velden 2018), we are bearing witness to an increasing variety of 'data activism' practices – a set of socio-technical tactics, resistances and mobilisations that adopt a critical approach towards datafication, mass data collection and pervasive surveillance. Data activism, as Milan conceptualises it, can be understood as a contemporary evolution of phenomena such as those analysed by Coleman (as well as Milan herself in previous works, e.g. 2013), like radical tech activism and hacktivism. Data activism is meant to represent the 'next step' in these forms of activism. It is both designed for the digital and shaped by the digital, inasmuch as it 'explicitly engages with the new forms (that) information and knowledge take today as well as their modes of production, challenging dominant understandings of datafication' (Milan and van der Velden 2018). Interestingly, the proponents of the concept point out that, given that datafication and the uses of ICTs for different political purposes are so widespread and pervasive, data activism might progressively acquire an appeal for more diverse communities of concerned citizens. This might extend beyond previous forms of tech activist engagement that seemed (self-)restricted to a niche of experts and technologists (ibid. 2018). Broadening the frame of, and interest in, tech activism is a widely discussed concern in a number of the most recent encryption projects, including some we will analyse more closely as this book unfolds.

Also relevant to our research, and key to understanding several of the dynamics described in the following chapters, is work that explores what it means to be a 'digital citizen' of the post-Snowden Internet. The conceptual lens of 'data justice' has been proposed by Arne Hintz, Lina Dencik and Karin Wahl-Jorgensen (2019) to illustrate that not only is citizenship and the possibility of citizen agency in today's Internet profoundly shaped by phenomena such as massive data collection and commodification, but also that user rights and practices concerning online privacy and surveillance are today conceived of in highly individualised terms. According to these authors, these individualising dynamics engender or at least maintain a context of inequality, as they transfer the responsibility to 'engage and negotiate citizenship in a digital age onto individuals' (Gangneux 2019).

As our case studies will illustrate, this issue is important in relation to encryption technologies and their mass adoption because the target audience of secure messaging applications either born or substantially developed post-Snowden is far from being limited to tech-savvy and activist groups: several projects are aimed at widespread use. This is a major change in the field, as for a long time, a majority of the technical crypto community considered that greater user-friendliness and usability could realise in practice their desire for large-scale adoption, while simultaneously considering ease of use and comfort a secondary issue to the soundness of the technology. Scholars have previously suggested that the comparatively little attention given to this issue by developers implies a 'forced responsibilisation' of users, as it places all the burden of 'getting up to speed' on them: it is up to users to acquire the competencies to compensate for the technical artefact's lack of usability. It has been further argued that this is to the detriment of the development of resilient collective digital security strategies (Kazansky 2015) and that it 'delegates' technical matters to 'progressive techies' despite a widespread societal desire to develop technologies for social justice (Aouragh et al. 2015).

Finally, we have found a particularly useful set of concepts within STS-focused studies of Internet governance (see e.g. Epstein, Katzenbach and Musiani 2016). Complementary to the predominantly institutional approaches that set the agenda for Internet Governance (IG) research in its early days – and which remain one of its preeminent features – STS approaches invite a consideration of the agency of technology designers, policymakers and users as they interact, in a distributed fashion, with technologies, rules and regulations. These, in turn, lead to consequences with systemic effects that may, at times, be unintended. Following these approaches, social and political ordering is understood as a set of ongoing and contested processes, which translates into a growing attention to the mundane practices of all those involved in providing and maintaining, hacking and undermining, developing and testing, or merely using the network of networks (Musiani 2015). Conceptually, STS-informed IG research relies on understanding governance as a normative 'system of systems' and it acknowledges the agency, often discrete yet pervasive, of both human and non-human actors and infrastructures. Particular attention is paid to the processes by which norms – technical or otherwise – are created, negotiated, put to the test and re-aligned, and also how they raise conflicts. These processes are understood to be as important as the stabilised norms themselves, if not more so. These are conceptual contributions that will be particularly relevant in the central chapters of the book, where we introduce the variety of architectural models that different projects choose to adopt initially and which they subsequently have to 'tinker with' due to factors including early user adoption, changes in the developers' teams and efforts to find suitable business models.

STS also provides crucial conceptual resources to enable the understanding of encryption as a site of controversy and contestation, in particular with the notion of sociotechnical controversy. On the one hand, since the very early days of the Internet, being on and managing the network of networks has been about exercising control over particular functions that provide specific actors with the power and opportunity to act to their advantage. On the other hand, there is very rarely a single way to implement these functions or a single actor capable of controlling them. Thus, the Internet is controversial and contested, both a target and an instrument of governance, and the object of interest of a myriad of actors: from the most powerful and centralised to the 'simple' Internet user (Epstein, Katzenbach and Musiani 2016). Infrastructural and architectural arrangements, the development and implementation of particular protocols, can be understood as a fundamental place to exercise economic and political power, as we have examined elsewhere (e.g. DeNardis and Musiani 2016).

The Internet exhibits an increasing number of sites of contestation. These include the interconnection agreements between Internet service providers (Meier-Hahn 2015), the debate around net neutrality (Marsden 2017), the use of deep-packet-inspection (Mueller, Kuehn and Santoso 2012), the deployment of content filtering technologies (Deibert and Crete-Nishihata 2012), ubiquitous surveillance measures and the use of DNS for regulatory aims (DeNardis and Hackl 2015), prediction of people's online behaviours via algorithmic governance (Ziewitz 2016) and the shaping of the visibility and hierarchies of search engine results (Mager 2012). Furthermore, contentious politics, activism and citizen-led protest are often embedded in the Internet and its applications. This is illustrated, for example, by Milan and ten Oever's (2017) work on civil society engagement within ICANN (which operates the Internet's Domain Name System), aimed at 'encoding' human rights into Internet infrastructures. Another illustration is our previous research on the shaping and use of citizen- and activist-oriented mobile and Web applications, and how the design of these tools shapes citizen participation and citizen-state interaction (Ermoshina 2016). Among all these examples, encryption technologies for online communications are becoming one of the core sites of 'governance by architecture', rife with controversies that concern, in turn, the development of these technologies, their implementation, their (sometimes surprising) appropriation by users and the attempts to regulate them.

Interestingly in this regard, Snowden's disclosures of 2013, and the subsequent widening of mass-surveillance-related debates, not only revealed a need for further legal reform of intelligence and surveillance systems but have also highlighted 'a variety of changing practices, policies and discourses that can (…) be related to post-Snowden contentions' (Pohle and Van Audenhove

2017: 2–3). A number of sociotechnical controversies can be related to this. A notable example was the FBI vs Apple controversy that spanned 2015 and 2016, when Apple Inc. received several orders by district courts in the United States to assist ongoing criminal investigations by extracting data from iPhones with extensive cryptographic security protections. Apple itself could not break this encryption unless it wrote specific new software to enable authorities to bypass such barriers. This debate notably questioned whether – and if yes to what extent – judicial or governmental authorities could compel technical manufacturers to provide assistance in unlocking devices protected by encryption systems (see also Schulze 2017). Controversies such as this have contributed to unveil facets of the *experience* of encryption in today's Internet and suggest that the most pressing issues of our time related to encryption may be not only legal and technical, but also social.

FOR A SOCIAL SCIENCES PERSPECTIVE ON (DE-)CENTRALISATION

As previously mentioned, the second core empirical and theoretical contribution of this book is intended to be the understanding of the social and political implications of particular design choices when it comes to the technical architecture of digital networks, in particular their degree of decentralisation (or lack of it). This issue, which has permeated the debates of both scholars and practitioners of networked technologies since their early days, in fact goes even further back in time. Indeed, the struggle between centralised, profit-driven systems and decentralised, user-controlled, user-innovated architectures is one that appears in many infrastructures and has been a longstanding concern of sociologists and historians of technology (see e.g. Edwards et al. 2007). In the early days of the telephone, people living in rural areas sometimes put together their own phone networks using barbed-wire fences as transmission lines; they were shared, distributed resources (Fischer 1987). The grand battle between trucking and rail in the United States was a duel between huge centralised systems (the railways) and independent entrepreneurs, often individuals, who used trucks to offer point-to-point (rather than station-to-station) delivery, and ultimately won by turning a publicly funded infrastructure (state and federal roads) towards a private purpose. Off-grid solar power installations as an alternative means of producing electricity outside standard circuits, and institutional resistance to these, are another case in point (Turner 2010). It is of little surprise, then, that the tension between different degrees of centralisation of technical architecture may also be found in the Internet, and in the different protocols and applications populating it – a tension that has been evident since its beginnings.

Indeed, in the history of Internet-based services, the concurrent push towards different types of design choice, in particular design based on peer-to-peer versus **client/server** architecture,[4] has for quite some time been a source of compromises and tension – including social, technical, political, economic and legal tensions (see Musiani 2015b). In a client/server architecture, having information stored not on a user's machine but a separate server, possibly one managed by a third party, greatly complicates resistance to censorship because it provides an obvious control point (DeNardis 2014) for authorities. On the other hand, without such a server, communication between users who are not permanently digitally connected becomes much more difficult. This is why core Internet services such as email usually resort to intermediaries that are able to ensure the ongoing functioning of the service but can also potentially stop it, limit it, block it, and read what passes through the servers they depend on (on the liability of Internet intermediaries for these actions see Riordan 2016).

Efforts aimed at developing decentralised systems date back to the early Internet (Minar and Hedlund 2001). They were generally built as ad-hoc strategic responses to specific threats of shutdown. The file-sharing system BitTorrent, for example, was developed as a response to the shutdown of Napster, in order to make legal prosecution for breach of IP in file sharing networks much more complicated (Izal et al. 2004). Napster had a peer-to-peer component in file search but was in fact being run by a small group of people. This implied that the system was fully dependent on these individuals, technically as well as legally. As a consequence, such systems can be effectively neutralised by turning off servers or seizing the equipment or the people in charge of them (Ku 2016). In contrast, decentralised systems do not have any central servers, and the functioning of the system involves many peers (people, and the computing resources at their disposal) who do not, or may not, even know each other. If any particular node is unavailable to the system, it continues to run regardless. Thus, the logic behind the creation of a decentralised system is usually to be resilient to targeting by authorities, and such systems are accordingly often deemed by technical and political actors in need of such resilience to be superior to proprietary, closed, more centralised systems, because they value long-term robustness over cost-effective commercial expedience (Oram 2001).

Decentralised systems have been subject to 'waves' of interest in the last twenty years, starting with the early 2000s file sharing frenzy and the hailing of peer-to-peer as a 'disruptive technology' (Oram 2001). In recent years there has been an even greater interest in and uptake of decentralisation. In the process, the motivations for adopting decentralised technologies have broadened from a particular strategy of opposition to specific companies or pieces of regulation, to proposals of an alternative 'vision' of what corporate, legal and state institutions should be. Two main dynamics have driven this tendency: the first is the emergence of blockchain technology (in particular with Bitcoin technology, as a response to the 2008 financial crisis; see Campbell-Verduyn 2017 and Brunton 2019), and the second was spurred by Edward Snowden's revelations of mass surveillance operations facilitated by a number of telecommunications companies and Silicon Valley giants, on behalf of the US National Security Agency (see Pohle and Van Audenhove 2017). These events greatly raised the general public's awareness of the surveillance-based, and personal data-based, business models of near-monopoly tech companies, and their 'dangerous liaisons' with state security agencies (Musiani 2013).

As a consequence of these dynamics, 'both decentralisation and the notion of authority took on broader meaning and decentralisation became a technical, political, economic and social aim in and of itself, reaching outside the 'hacker' circles of the early p2p systems' (Brekke & Isakiidis 2019). However, this larger appreciation of decentralisation as a principle and a vision is not devoid of side effects; most notably, often decentralisation has become an objective in and of itself, with little understanding of intent or assessment of actual effects. As information studies scholar and Internet pioneer Philip Agre said in 2003, 'architecture is politics, but should not be understood as a substitute for politics'; decentralised protocols are too readily assumed, because of their technical qualities, to bring about decentralised political, social and economic outcomes. By choosing to structure the central part of this book around the different degrees of centralisation of the technical architecture for the examined secure messaging systems, we intend to take Agre's lesson seriously, and assess in detail the extent to which economic, social, legal (and last but not least technical) factors complicate the picture of a linear 'translation' from a peer-to-peer technical architecture into a successful decentralised socioeconomic system, or from a centralised technical model to a top-down sociopolitical structure.

CASE STUDY SELECTION

The core of this book is an in-depth understanding of three different end-to-end encrypted mail and messaging applications. After a preliminary survey of thirty cases of encrypted messaging applications,[5] we proceeded to select a few of them for more detailed study. These three applications were selected based on their underlying protocols, and because of the relative accessibility of the developer communities for interviews and observations. The three applications originally selected were Signal (a centralised end-to-end encrypted instant messaging application), LEAP/Pixelated (a federated end-to-end encrypted asynchronous messaging protocol and client) and Briar (a peer-to-peer end-to-end encrypted messaging application for resilient communication using **network-layer protection**, such as Tor hidden services).

These three cases offered the possibility to address various research questions, such as the motivations behind:

- particular architectural choices (centralised, federated or peer-to-peer);
- specific choices of licensing, **UI/UX** design, relations between the underlying protocols and the application level;[6]
- solutions to privacy properties (such as metadata protection);
- design choices for group communication;

- various approaches to security properties (forward and future secrecy; **server-side archives**; **cryptographic deniability**; ephemeral or disappearing messaging).

However, when in September 2016 we started our fieldwork on the three selected projects, we quickly understood that these projects could hardly be treated as discrete given their connections with other initiatives in the field of encrypted messaging and email. In fact, the underlying protocols used by these three projects gave birth to a number of **client-side implementations**, forked or actively interacted with various applications in the field. Thus, we decided to 'follow' the three projects as they grew and transformed and use them as our 'threads of Ariadne', respecting the loops and knots that these threads were naturally forming on their way. During our fieldwork we had the opportunity to meet and talk with a large number of professionals, ranging from cryptographers to UI/UX designers, trainers and users, about the protocols and tools we focus on here (in discussions both recorded and off the record).

The research work subtending this book was and is thus an attempt to tell the complex story of protocols and communities, and eventually, to approach questions of governance of encryption protocols. Through a comparative analysis of centralised and decentralised protocols and their implementations, we address here several important and broader questions: What are the architectural patterns of successful centralised and decentralised systems? How do developers go about building scalable and high-performing privacy-preserving decentralised architectures? Can decentralisation help deliver privacy and anonymity? What are the motivations, values and characteristics of user communities that lead to the success or failure of certain (de-)centralised systems?

A NOTE ON METHODOLOGY

Grounded in the different strands of literature from STS and the other disciplines we introduced above, our approach can be described as a multi-sited ethnography, inasmuch as we have undertaken research in, and between, several online and offline locations as part of our study, and we have also explicitly conceived specific technical protocols and systems as ‘part of a larger context that exceeds the boundaries of the field site’ (Muir 2011: 1015; see also a reflection on the method by its first proponent, George Marcus, who points out that multi-sited ethnography has been ‘most creative, critical, and interesting where it has been involved with the [STS] study of distributed knowledge systems, (Marcus 2012: 27).

We analyse the development of the architectures and the interfaces of messaging apps as ‘meeting points’ between the intentional goals of developers and the needs of users (Oudshoorn and Pinch 2005), In doing so, we aim to provide a fieldwork-driven explanation of emerging systems and communities of practice through ‘analytical thick descriptions’ (for a recent treatment of the concept, first introduced by anthropologist Clifford Geertz, see Ponterotto 2006) of events, artefacts and organisations. In particular, we pay attention to moments of crisis, debate and controversy – to try and understand the life of a technical artefact, from its creation to its appropriation and reconfigurations by users, to its becoming a subject of public debate, of governance, of lobbying. The primary methodology to achieve this goal has been to observe, for relatively prolonged periods of time, specific case-study groups or communities, while on the side conducting in-depth interviews with their members and reading appropriate documentation such as release notes and accounts of working sessions.

Just as we seek a nuanced understanding of developers’ motivations and the representations they have of users and their needs, in the tradition of ‘user studies’ developed within STS (see Oudshoorn and Pinch 2005 or, in the French tradition, Jouët 2000), we understand users not as a homogeneous and passive group, but as active participants in innovation and co-shaping technologies. In software development, this is possible via routes such as bug reporting, **pull requests** on code, mailing list comments and in-person contact between users and developers.

Among our interview subjects, developers were mostly selected on the basis of pre-existing personal relationships that the NEXTLEAP research team members had with the cryptographic research community. For projects with which research team members did not have any previous personal connections, we also reached out to developers via the GitLab and GitHub pages of the projects (e.g. Ricochet, Conversations). In contrast, user studies tended to be conducted with individuals selected through their attendance at training events in their local environments (both high-risk, in the case of Ukraine and Russia, and low risk in the case of France, Germany, Austria and the United Kingdom).[7] Our selection of events and conferences to attend was driven primarily by our interest in speaking to users from high-risk contexts. Indeed, while the inclusion of high-risk individuals was important for the project (as Chapter 1 will show), due to the level of repression these users face in their native environment, it would have been difficult if not impossible to interview them there, since they would be unable to speak openly. This was the case for users from Egypt, Turkey, Kenya and Iran, where the interviews took place in March 2017 at the Internet Freedom Festival and at RightsCon. All interviews were conducted between autumn 2016 and the late summer of 2018, with 63 interviews in total. At several of these gatherings and training events, we also asked our respondents to take a moment to provide us with a drawing or a graphical representation of what/who they considered to be their security threat or adversary when it comes to digital communications. These images proved to be a very fruitful addition to our fieldwork materials, as Chapter 1, in particular, will show.

Throughout our research, and due to the sensitive nature of our subject vis-à-vis online civil liberties, it was important to keep questioning the modalities of our access to fieldwork, and to be continually reflexive about our core assumptions and the ethical guidelines we as researchers were working with – questions that have been identified as particularly relevant when issues of secrecy, privacy and security are at play (Barbosa and Milan 2019; De Goede et al. 2019; see also the Appendix to this book).

Being the 'useful sociologist' in a team of technologists

The fieldwork behind this book was a journey through disciplines, fields of expertise, methodologies and communities – an experience of professional and sometimes personal transformation for us as researchers, that led to a redefinition of our role as sociologists within a tech-oriented project. The NEXTLEAP team was a consortium of six partners: four were research teams based at academic institutions (three in computer science, one – the authors of this book – in sociology), one was a research centre whose activities include a mix of philosophy-inspired action research and outreach to civil society and institutions, and one was a software development firm. Thus, the team was far from being exclusively composed of academics, and STS academics were a definite minority.

We, the authors of this book, come from what is often considered as 'the temple of actor-network theory':[8] the Center for Sociology of Innovation, based at the MINES ParisTech school of engineering in Paris We therefore initially approached our research on secure messaging as a challenge for STS. Our initial academic desire was to target the work of technical actors – developers and protocol designers – and the encryption protocols themselves. However, after we delivered the first state-of-the-art description of end-to-end encrypted messaging applications and protocols, we faced a clear demand from other members of the research team: 'focus on users'. The following months of fieldwork were marked by several interactions between us and the technologists in the team, and ultimately led to an important redesign of our interview guide. At times we were also asked to revise our research questions and priorities to include a clearer focus on insights from user-oriented interviews. Eventually, we came to understand how we looked to the rest of the team: when software development cycles include a non-technical role, this role is usually that of the 'usability researcher', a place that had been, somehow, automatically reserved for us.

Thus, the story behind this book is also a story of two STS researchers defining their own role within an interdisciplinary team, not without a certain amount of tension. The attempts to convey to the technologists what our STS approach was, and how it could actually be useful for them and their development process, despite not being straightforward user studies, eventually led us to develop our own 'circumvention techniques' to make collaborative work possible.

Embodying the 'useful sociologist' in a team of technologists, we found ourselves between fields, something that is also reflected in our previous publications related to the project. We found ourselves presenting our work at conferences on usable security, publishing our works in computer science reviews focusing on usability studies, side-by-side with usability researchers. However, we maintained a connection with the STS world through a thin but, we believe, robust thread of reflexivity, as we developed a critical attitude to our own usability alter-ego and managed to use it as a key that helped us penetrate the otherwise quite hermetic world of crypto protocol design. While, by consortium design, our interactions and collaborations with our primarily technical colleagues were frequent and close, this book is most definitely, in retrospect, a way to tell the story of our three-year investigation that is intimately our own, departing when necessary, from the compromises needed throughout the project to produce results and publications driven by the conventions of both computer science and the social sciences.

The first step in this process was perhaps the Autocrypt[9] gathering in Berlin, in December 2016, where Ksenia was invited to talk about 'user needs and desires' for encrypted email and messaging and develop 'use-cases' that could potentially be helpful in the design of the new specifications for email encryption. This event became the true starting point for our fieldwork – a gathering of some of the most advanced cryptographers and developers, working on projects such as Matrix.org, Enigmail, Wire, Secure Scuttlebutt, LEAP, Riseup and others. At the end of the day, the rest of the NEXTLEAP research team's 'hunt for the user' had finally brought us to the heart of ongoing development and protocol design work.

Thus, this book is an occasion to reflect upon our work as an example of embedded real-time STS, where researchers are active participants in techno-scientific work involving multiple stakeholders and contingencies. Throughout our case studies, we describe several examples of how our research fits into protocol design work, and occasionally reflect upon tensions within the research team. Ultimately, the desire to 'meet the user', that shows through the work of our technical colleagues, tells us something about the evolution of encrypted messaging towards a more human-centric design, reflected in recent developments among certain Internet governance standardisation bodies, such as the IETF (Internet Engineering Task Force) and its research branch IRTF (Internet Research Task Force), that seek to include human rights considerations in protocol design (see ten Oever 2021).

Before we present the structure of the book, and in order to facilitate navigation through the chapters that follow, the last part of our introduction will present a genealogy of the fundamental protocols in the encrypted messaging field; in it, we introduce relevant concepts and definitions that will be used in the following chapters.

Encrypted messaging protocols: The short genealogy of a 'feedback loop'

The most recent generation of tools for secure communications (appearing in the 2010s, in particular post-Snowden) marked the rise of encrypted secure messaging 'for the masses'.[10] Yet despite this recent success vis-à-vis the general public, encrypted messaging is an unstandardised and fragmented field, as developers remain in a state of flux about how to implement security and privacy properties. In particular, developers face a number of trade-offs between various design issues, including security and privacy properties, the introduction of group support features, the degree of decentralisation of the application, and standardisation and licensing attempts. To attempt an initial systematisation of this complicated landscape, our first step was an in-depth survey of thirty email and chat applications offering end-to-end encryption.[11] As part of this, we analysed their architectural and protocol choices, as well as their interfaces and business models (see also Ermoshina, Musiani and Halpin 2016). As an introduction and contextualisation of our research subject, this section provides a historical look at the development of email and secure messaging protocols in the light of cryptographic and usability problems that these protocols have sought to solve, while introducing relevant concepts and definitions that will be used in the following chapters. This brief, non-linear history of protocols and applications that have recently built the field of secure messaging is also a first look at an issue which we will further develop in the coming chapters: the technical and organisational choices made by protocol designers and app developers are, in fact, enacting various forms of freedom, both for users and developers.

End-to-end encrypted messaging is increasingly prominent, with its adoption by large proprietary applications such as WhatsApp and Facebook Messenger. In 'end-to-end' encrypted messaging, the server that hosts messages for a user or any third-party adversary that intercepts data as the message is *en route* cannot read the message content due to the use of encryption. The 'end' in 'end-to-end' encryption therefore refers to the 'endpoint', which in the case of messaging is the client device of the user rather than the server.

After the Snowden revelations, the academic cryptographic community has, with renewed impetus, sought to rigorously engage with the '**untrusted server**' problem. This is an issue that until recently had felt, as suggested by Phillip Rogaway, 'almost intentionally pushed aside', although it is perhaps 'the most fundamental privacy problem in cryptography: how can parties communicate in such a way that nobody knows who said what' (Rogaway 2015). The so-called 'new generation secure messaging protocols', such as Signal's **Double Ratchet**, seek to address these issues and provide a remedy for the security and privacy flaws identified in older protocols, such as OTR or PGP. The success of the Signal protocol, widely forked and adopted by many secure messaging projects, has catalysed debates within cryptographic communities, and led to the revival and renewal of older protocols, creating a 'feedback loop' effect. Thus, the genealogy presented here challenges linear histories of secure messaging protocols, as it unveils dynamic iterations between recent and older protocols, as well as between what was considered 'synchronous' versus 'asynchronous' protocols.

Email encryption

Historically, email has been considered a form of asynchronous messaging, where a user does not have to be online to receive the message, while chat is considered to be a form of asynchronous messaging, where a user has to be online to receive the message. However, these distinctions are increasingly blurring now that popular chat protocols generally support asynchronous messaging, and the email protocol is more and more often used for instant messaging, with the rapidly evolving galaxy of **chat-over-email** projects (see Chapter 4). Email is now considered a possible infrastructural solution for projects seeking not only privacy and security but also **interoperability** and some resistance to censorship.

Email is based on standardised and open protocols that allow interoperability between different email servers, so that, for example, a Microsoft server can send email to a Google server. SMTP (Simple Mail Transfer Protocol) is the protocol originally used for transferring email and as such is one of the oldest standards for asynchronous messaging, first defined in 1982 by the IETF[12] (Unger et al. 2015) and by default not including provision for content confidentiality. Classically, as the NSA's PRISM program has eloquently revealed, email is sent unencrypted and so the server has full access to the content of email messages. The federated nature of email infrastructure makes this even more problematic, as trust in service providers within decentralised systems is hard to guarantee. Thus, developers have for a long time made clear their intention to progress towards usable methods of end-to-end encryption for email.

To add end-to-end encryption capabilities to email, the PGP (Pretty Good Privacy) protocol was created in 1991 by Phil Zimmerman, as an ambitious technosocial attempt to 'preserve democracy' and let people 'take privacy in their hands.[13] Due both to pressure from the US government and patent claims by RSA Corporation, Zimmerman pushed PGP to become an IETF standard. The OpenPGP set of standards was finally defined in 1997, to allow the open implementation of PGP. GPG (GnuGPG) is a free software implementation of the OpenPGP standards developed by Free Software Foundation in 1999 and compliant with the OpenPGP standard specifications, serving as the free software foundation for most modern PGP-enabled applications.

OpenPGP is implemented in both desktop and mobile email apps, including Outlook, Apple Mail and Thunderbird through plug-ins. An alternative standard for encrypted email, called S/MIME,[14] is also supported via plug-ins by most major email clients. The main difference between OpenPGP and S/MIME is that the latter requires the installation of certificates provisioned by centralised certificate authorities. In contrast to PGP, which is based on a decentralised 'Web of Trust' between users who accept and sign each other's keys (and therefore delegates the responsibility of the complexity of **key management** to the end-user), S/MIME uses a centralised **public key infrastructure** to manage keys. Thus, while it has been adopted by some large, centralised institutions, it has been much less frequently adopted by the general public. In contrast to centralised approaches, OpenPGP offloads the key management to the users via a decentralised 'Web of Trust' model.

OpenPGP and S/MIME also work on mobile devices, such as PGPMail, but as OpenPGP binds the key to the particular device, there have often been concerns about how to securely transport any long-term private key material between devices, and so mobile adoption of encrypted email is considered to be low among users and problematic in terms of security. Although the challenges of using PGP on mobile platforms are well known, mobile PGP has not been subject to usability studies in the same manner that PGP itself has. S/MIME has been tested in some usability studies and in general demonstrates better usability than PGP, insofar as key management does not have to be maintained by the end-user, but users still have trouble understanding the interface.

In general, PGP was considered to have poor usability as users could not understand key management and judge how cryptographic keys establish trust relationships, or even understand the interface. These problems extend to security: if an adversary compromises a user's private key, this allows all encrypted messages to be read. While there has been a resurgence of interest in OpenPGP since 2013, it has not been deployed to any great extent by ordinary users due to the aforementioned issues. In 2015, the IETF reopened the OpenPGP Working Group[15] in order to allow the fundamental algorithms to be upgraded and to use more modern cryptographic **primitives** (for example, support for new algorithms).

The underlying PGP protocol presents a number of well recognised flaws. First, PGP tends to allow any and every combination of uses of encryption and signatures based on user preference, but does not offer authentication of the **headers** (i.e. the 'to' and 'from' fields). This allows messages to be surreptitiously forwarded and otherwise redirected. In general, PGP has been considered an open standard that has serious problems in terms of both security and usability, and this prompted the rise of a generation of competing technologies such as Off the Record Messaging. However, recently, the email community has been quite active and has developed a number of initiatives that have sought to renew PGP and to 'make email encryption great again', as Delta Chat's lead developer and former NEXTLEAP member, Holger Krekel, summarised during a conversation with us. The result is that, since 2016, the PGP community has experienced a definite revival through the introduction of new solutions such as Autocrypt, which automates both secret and public key management by adding an Autocrypt-specific mail header to outgoing mails which contains, among other information, the sender's public key.[16]

Instant messaging encryption

Unlike email, which started as a high-**latency** and asynchronous messaging system, chat protocols began as low-latency synchronous messaging, although recently the line has become increasingly blurred as many chat protocols allow asynchronous message delivery. The user patterns of chat apps have also become increasingly varied in recent years, questioning the distinction between social media and messaging platforms ('messaging is the new social media […] families use WhatsApp groups instead of Facebook'; Balive 2015).

The development of encryption for chat apps corresponded to changes in the contexts of usage (notably the move from desktop to smartphone technologies) and the spread of mobile Internet. The first encryption protocol for instant messaging, called OTR (2004), presumed a synchronous setting with both contacts being online at the same time. The birth of the second important protocol for end-to-end encryption protocols (Axolotl, started in 2013, now called Signal protocol) corresponded to the rise of instant messengers (in 2013, chat apps surpassed short message services in global message volume for the first time; see eMarketer 2015) and to the Snowden revelations.

The most widely used standardised chat protocol is called **XMPP** (Extensible Message and Presence Protocol) and it became an IETF standard in 2004. XMPP is a federated standard that 'provides a technology for the asynchronous, end-to-end exchange of structured data […] among a distributed network of globally addressable, presence-aware clients and servers' (Borisov et al. 2004). There are many implementations of the XMPP specifications, with the XMPP Foundation giving a list of 35 clients, 12 servers and 15 libraries using the XMPP protocol.[17] XMPP traffic and content are not encrypted by default, although network-level encryption security using **TLS** has been built into the core. In addition, according to the XMPP foundation, a team of developers is working on an upgrade of the standard to support end-to-end encryption.[18]

The OTR (Off-the-Record) protocol, released in 2004, is an extension to XMPP to provide end-to-end encryption. In their paper with the iconic title 'Off-the-Record Communication, or, Why Not to Use PGP', the creators of OTR, Borisov and Goldberg, describe their protocol as a security upgrade of PGP, at least insofar as it does not have long-term public keys that can be compromised. OTR also provides deniable authentication for users, unlike PGP messages, the latter of which can be later 'used as a verifiable record of the communication event and the identities of the participants' (Borisov et al., 2004). The first OTR implementation was a popular Linux IM client, GAIM. At the present moment it is said to be used by 14 instant messaging clients,[19] including earlier versions of Cryptocat (in-browser Javascript client), Jitsi, and ChatSecure (XMPP client for Android and iOS). However, the first versions of OTR were designed for synchronous messaging between two people, and so did not work for group messaging or asynchronous messaging.[20]

The Signal Protocol, the non-federated protocol developed in 2013 by Open Whisper Systems, is said to have evolved in response to the flaws and limits of OTR. Moxie Marlinspike, the co-author of Signal, was inspired by some features of OTR, such as the idea of **ephemeral key exchange** (Marlinspike 2013), but also added additional security features such as future and forward secrecy, support for asynchronous messaging and group messaging, going a step further than OTR by allowing clients to be offline. The Signal Protocol is used in mobile messaging applications such as the homonymous Signal (formerly TextSecure and RedPhone) and WhatsApp, while its forks are used in Wire and Riot. Silent Circle, a Washington, DC-based encrypted communications firm founded in 2011, has used a version of the Signal Protocol since 2015 in its Silent Phone. In 2016 Facebook announced the implementation of Signal Protocol for Facebook Messenger.[21]

Regardless of these multiple re-usages and forks, the Signal Protocol remains unstandardised, as we will explore in Chapter 2. However, the first step towards 'standardisation' of parts of the Signal Protocol has begun with the creation of **OMEMO** (a recursive acronym for 'OMEMO Multi-End Message and Object

Encryption'). OMEMO is a new encrypted extension of the XMPP protocol developed in 2015 that effectively copies the Signal Protocol and adopts it to XMPP. It was presented to the XMPP Standards Foundation in 2015 but is still in its experimental phase.[22] OMEMO builds upon the work of the Signal Protocol, responding to the flaws of both OTR and PGP, due to OTR's 'inter-client mobility problems' and the absence of forward secrecy of OpenPGP and its vulnerability to so-called replay attacks. The software implementations of OMEMO are growing, and include Conversations, an open-source application for Android that counts over 50000 downloads via Google Play Market, and an unknown number of installs via F-Droid.

Network-level anonymity

End-to-end encryption does not usually allow a user to be anonymous to the server or a third party without additional network-level encryption. Thus, network-level initiatives, such as P2P routing services or anonymous remailers, which can add supplementary privacy properties to end-to-end encrypted messaging, are worth mentioning here. Metadata protection and traffic obfuscation is still an area of active research, stimulating experiments with standards and architectures (e.g. Vuvuzela's usage of 'noise' to obfuscate metadata, discussed in Van den Hooff et al. 2015). There seem to be no functional standards on this level yet; however, some solutions, such as Tor or I2P, tend to serve as references or *de facto* standards for different projects.

The Tor hidden service protocol offers a platform to develop decentralised and encrypted instant messenger servers. Tor (the name is derived from the acronym of the original software project, 'The Onion Router'), is software that directs Internet traffic through a network of volunteers, globally dispersed, which act as relays to conceal a user's location and usage, essentially making it more difficult for a third party to trace Internet activity to a particular user. Tor's success and fame mostly relies on its ability to provide privacy and anonymity to vulnerable Internet users. It is used as a default by projects such as the Tor Messenger, Pond and Ricochet. Another example is the decentralised and end-to-end encrypted mobile messenger Briar, which relies on the Tor network when available, but could also work over Bluetooth in case of emergency off-the-grid situations. Briar is described in more detail in Chapter 3.

Tor only provides anonymity for network addresses, but not metadata such as the sender, recipient and time of message, which are kept in the email header at the time of email or can be deduced by the server. Historically, work has been carried out on anonymous high-latency remailers to fix these transport metadata leaks in federated messaging, these falling under three types: Cypherpunk Anonymous Remailer, Mixmaster and Mixminion. The last of these is not currently active, according to the project's website.[23]

A number of experimental network-level tools, while not guaranteeing anonymity, provide some level of encryption. Zero Tier One is an end-to-end encrypted, peer-to-peer virtual network that provides static network addresses which remain stable even if the user changes physical WiFi/networks. CJDNS implements a virtual **IPv6** network in which all packets are encrypted to the final recipient, using **public key cryptography** for network address allocation and a distributed hash table for routing.[24]

A fragmented yet vibrant field

As we observed in previous mapping research on P2P services (Méadel and Musiani 2015), part of the reason why there is such great diversity and complexity in this field is the relatively short lifespan of several projects. While our mapping of thirty end-to-end encrypted messaging and email apps covered only projects that are currently active (with one exception, Pond, 'in stasis', albeit not deactivated), our preliminary research revealed countless others that, after two or three years of pre-beta phase, and sometimes less, stopped development with no evident explanation. While in more than a few cases, the motives behind this are primarily related to technical experiments that did not deliver as hoped or expected, a number of additional factors may also be responsible, including the failure to develop an economic model, the internal governance of FOSS development groups, and the inability to rally a critical mass of users around the app (possibly due to a lack of ease-of-use, as discussed below).

Despite the prevalence of free and open-source software projects, proprietary software is not absent in this landscape, revealing both a potentially fruitful 'business-to-business' market for end-to-end encryption and a lack of open-source and standards adoption by mainstream applications. Open source itself is multi-layered and sometimes hybrid, with the code on the client side being open source and the server side being proprietary. Perhaps unsurprisingly, the proprietary features are more important in applications destined for business-to-business use. Free and open-source software is predominant for tools adopted or designed to be used by activists and tech-savvy users. The transparency of code and encryption protocols used by open-source software is aimed not only at improving the project, but also at producing communities of peer reviewers, experts, beta-testers and advanced users who participate in a collective reflection on the future of privacy-enhancing technologies.

The target audience of the applications is far from being limited to tech-savvy and activist groups; several projects are intended for widespread use, and user-friendliness appears to be the main issue that stands between this wish and its realisation. A look at visual aspects connected to applications – the design of interfaces, for example, or the design of diagrams and graphics to explain the functioning of the applications – also reveals the different publics targeted by applications and how the developers perceive them. General public-oriented systems use very 'politically neutral' imagery, resorting to the very classical 'Alice and Bob' models[25] while stressing that their tools are for 'everyone' (e.g. for 'sharing holiday photos'), while tools meant for companies emphasise in both visuals and words a focus on security. Other narratives refer to fictional anarchist leaders or real-life activists (e.g. 'Nestor Makhno' or 'Vera Zassulitch'), figures likely to resonate with the target audience. Interestingly, in some instances where user feedback is visible on the App Store or Google Play, it shows that end-to-end encryption is perceived as problematic because both sender and receiver have to install the app for encryption to take place, which complicates usage.

Several secure messaging projects propose solutions to the problem of data storage. Indeed, despite the guarantees of 'no personal data collection', some projects still store key data on the servers (such as usage statistics, device information, keys, usernames or friend relations). Developers tend to explain such practices by reference to technical requirements (e.g. proposing a better user experience based on the usage statistics collected) but many developers remain keen to seek alternatives that involve minimal data storage and use stronger forms of decentralisation.

A related issue is a powerful 'double' narrative about end-to-end encryption. If on the one hand, it is associated with a very strong discourse on empowerment and the better protection of fundamental civil liberties, several projects show in parallel a desire/need to defend themselves from associations with criminal activity and allegations such as 'encryption is used by jihadists' (Sanger and Perlroth 2015). Such narratives are fuelled by previous and current ones about decentralised technologies and peer-to-peer, with their history of alleged 'empowering-yet-illegal' tools. These issues in turn connect to the broader context of discussions about governance by infrastructure and civil liberties (Musiani et al. 2016), some of them particularly related to encryption (or the breaking of it), such as the Apple vs FBI case[26] and WhatsApp using, since April 2016, encryption by default. Thus, the present research hints at something that we will address in the following chapters – something a large majority of the projects need to take into account, and indeed are already taking into account: architecture is politics, but not a substitute for politics (Agre 2003).

Given the range of debates, controversies and emergent publics around encryption and secure messaging, we hope to have begun to show why a social perspective is necessary for the design and refinement of technical protocols. This includes the necessity to understand how and whether users understand and value the various security properties of the protocols. For example, how do users understand what is a 'key' or what is 'forward secrecy'? Often, protocol designers make assumptions about whether or not 'ordinary users' can understand the security and privacy properties of their protocols. For example, almost all protocols from PGP to Signal use methods such as 'out-of-band fingerprint verification' to determine whether or not the recipient of their message really is who they think they are. Our research shows that users rarely actually use these techniques to verify the identity of their contacts.

Another example that has been debated in the technical community is deniable authentication. While a protocol may be technically deniable, would this cryptographic deniability be able to stand the test of society, for example in a court of law? Answering these kinds of questions influences the kinds of protocols that can be designed by the research community. Lastly, why do only some protocols enable decentralisation via **open standards**? Do only specific groups of users (tech-savvy and activists) have a strong preference for peer-to-peer or federated solutions over centralised services? This book hopes to address these and other related questions.

STRUCTURE OF THE BOOK

Over the course of the next six chapters, the overall objective of the book is to provide an analytical portrait of the field of encrypted secure messaging, in order to explore the experience of encryption in today's variety of secure messaging protocols and tools, and their implications for the making of digital liberties.

The field of encrypted messaging offers many solutions designed to conceal, obfuscate and disguise private communications and other online activities. These solutions are tailored to protect against specific 'adversaries'. The security and privacy features worked into different protocols offer various degrees of protection and let users conceal different parts of their online identities. To illustrate this, Chapter 1 shows how instruments such as 'threat modelling' and risk assessment are deployed during the development of tools in order to either identify from whom a user needs to hide or to analyse the possibility or chance of a threat being realised. Also, it becomes important not only to know who to conceal from, but also to evaluate the chances of actually 'meeting' this adversary. In fact, users perceive themselves as having, not a single identity, but rather a set of profiles or personas: daughter, journalist, lover, activist, colleague… Each role, according to users, may require a specific form of digital self-care or a specific set of tools. Each persona implies a specific pattern of online behaviour, thus creating what is called 'security by compartmentalisation'. A consequence, as we argue in Chapter 1, is that when applied to online privacy and security, risk is a relational and socially defined concept, as it greatly depends on the user's social graphs and communicative contexts.

Chapter 2 moves into the more empirically focused part of the book, by examining the case of a centralised application – Signal – and its underlying eponymous protocol. The Signal protocol is now considered to embody 'best practice' in the field of encrypted messaging and has become a trend-setter for other projects in terms of privacy and security features. Currently, Signal is centralised, as a single server mediates the setup of the protocol in its most widespread deployments. A new means of 'quasi-standardisation' or 'standardisation by running code' is being practised around this protocol. In this process, a quasi-standard is defined as 'something that works' and is iterated and redeployed by others. Centralisation has allowed Signal developers to update the protocol rapidly enough in response to research and bugs, and to limit concerns about the technical competence of having third-party developers potentially adapting their protocol to other applications than their in-house one. However, the 'bottleneck' of centralisation also implies that difficulties and tensions have arisen in connection with some attempts to reimplement the Signal protocol, due to the lack of clear guidelines and specifications in order to do so. Chapter 2 discusses centralisation as a 'control by design' model – in particular, control over changes in the protocol, so as to respond quickly to technical challenges. Here the chapter draws on two other cases alongside Signal: Telegram and Wire.

Chapter 3 examines peer-to-peer based secure messaging applications. Particular populations of users, especially those living in 'high-risk' environments, show interest towards these decentralised systems, as they see an alignment between their own favoured political and economic models – based on the principles of horizontal connections, mutual assistance, self-governance, participation – and the technical architecture of distributed networks. Peer-to-peer, as with previous recent instances, also promises less control by both governments and private corporations. However, peer-to-peer encrypted messaging faces a number of technical challenges, including a 'vicious circle' between adoption barriers and a dependency on a critical mass of users, the difficulty of managing users' reputations and identities (identities are unique but users usually find them hard to memorise due to the form they are presented in), placing trust in the client (which presents many advantages censorship-wise but may present risks for users living in authoritarian regimes, where the main threat model remains physical pressure and device seizure). By discussing, in particular, the case of the application Briar and its underlying protocol, this chapter analyses both the potential and the challenges of decentralised architectures as applied to encrypted messaging.

Chapter 4 completes the analysis of different architectural choices and their impact on the configuration of encryption tools by examining systems based on federative models. When it comes to communities of developers debating online, the tensions between centralisation and more distributed architectural forms, such as federation, go hand-in-hand with debates over standards. Federation can help alleviate and distribute the very high degree of personal responsibility held by a centralised service provider and favours the freedom of users to choose between different solutions. On the other hand, it can present problems in terms of security, as it is harder to audit all the different implementations of a federated protocol and ensure correct updates. Drawing on the examples of Conversations (and its underlying OMEMO protocol), Matrix.org, and LEAP/Pixelated, Chapter 4 retraces the debates on federation in encrypted messaging, and analyses how federation takes shape in these debates as both an infrastructural configuration and a social experiment, in each case seeking a compromise between more distributed architectures and high levels of security.

Given the great variety of encrypted messaging solutions, how is one – a user, an NGO, a professional – to make sense of them? Chapter 5 tells the story of one such attempt. Classifications and categorisations are, to put it in Bowker and Star's (1999) words, 'powerful technologies', whose architecture is simultaneously informatic and moral and which can become relatively invisible as they progressively stabilise while at the same time not losing their power. Thus, categorisation systems should be acknowledged as a significant site of political, ethical and cultural work. This chapter examines such work as it relates to encrypted messaging tools, by examining, in particular, one of the most prominent initiatives in this regard: the Electronic Frontier Foundation's 2014 release of the Secure Messaging Scorecard (SMS). A particular focus is on the debates it sparked, and its subsequent re-evaluation and evolutions. We show how the different versions of the SMS, as they move from an approach centred on the tools and their technical features to one that gives priority to users and their contexts of use, actively participate in the co-shaping of specific definitions of privacy, security and encryption that put users at the core of the categorisation system and entrust them with new responsibilities.

Finally, the concluding chapter of the book ties together insights from the previous chapters to reflect on encryption as a site of social, political and technical controversy. Issues related to encryption and its adoption in messaging systems are inextricably entangled with issues of standardisation (formal/informal), the political economy of software development and adoption, and choices of technical architecture. This concluding chapter will offer some reflections on these different aspects as they have been informed by our fieldwork and will then tie the diverse ways in which political effects can be achieved through technological choices to broader political concerns related to privacy, examining in particular how they can interact with recent supra-national legal instruments such as the General Data Protection Regulation (GDPR). Finally, we will comment on the implications of our study and of cognate research for the development of social studies of encryption and for its interactions with Internet governance research, in particular of STS inspiration.

We now move into the first chapter of this book, written from the standpoint of users and security trainers – encrypted messaging experts working in an intermediary zone between developers and users. We will follow them as they deploy various strategies to make sense of the complex and moving ecosystem of end-to-end encrypted messengers.

NOTES

[1] For example, future secrecy, which we will address in detail later in the book.
[2] Following up on previous work by the authors (e.g. Musiani 2015b).
[3] Scholarly and non-scholarly debates about the term ‘hacker’ are ongoing. For the purpose of this book, and given that several projects and tools examined in it do not necessarily refer to an imaginary of subversion, we follow Hellegren’s (2017) definition of a hacker as a member of a community that unites with like-minded members ’in their practices of developing and modifying internet-specific technologies’.

[4] Many Internet protocols are client/server, which means that the machines that communicate are not equivalent: one is a server, permanently on and waiting for connections; the others are clients, who connect when they have something to ask. This is a logical mode of operation, for example, in the case of the Web: when you visit a website, you are a reader, and the entity which manages the website produces the content you seek to read. But not all uses of the Internet fit into this model; they include direct sending of messages, or file exchanges – not a one-way communication but a peer-to-peer one, with two machines or two humans communicating directly.

[5] This work is available as deliverable 3.1 of the NEXTLEAP project.

[6] The three cases develop both a user-facing client application and a protocol that can potentially be separated from it (Signal protocol, LEAP and Bramble respectively).

[7] We will come back to the high-risk/low-risk distinction, its opportunities and shortcomings, in Chapter 1.

[8] We frequently get this type of remark from STS conference attendees.

[9] Autocrypt will be extensively presented in Chapter 4 as an example of a federated-architecture encrypted messaging system.

[10] A previous version of this section was published as Ermoshina, K., F. Musiani & H. Halpin, 'End-to-end encrypted messaging protocols: An overview', in Franco Bagnoli et al., eds, *Internet science. Third international conference, INSCI 2016, Florence, Italy, September 12–14, 2016, Proceedings*, Springer, p. 244–254.

[11] The thirty applications we examined are: Briar, Caliopen, ChatSecure, CoverMe, CryptoCat, Equalit.ie, GData, i2P, Jitsi, Mailpile, Mailvelope, ParanoiaWorks, Patchwork, Pidgin, Pixelated, Pond, Protonmail, qTOX, Ricochet, Scramble, Signal, SilentCircle, SureSpot, Teem/SwellRT, Telegram, Threema, Tor Messenger, Vuvuzela, Wickr, Wire.

[12] https://tools.ietf.org/html/rfc821.

[13] https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

[14] See, e.g., https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/s-mime-for-message-signing-and-encryption?view=o365-worldwide.

[15] https://datatracker.ietf.org/wg/openpgp/charter.

[16] See Chapter 4. Also, https://autocrypt.org/level1.html#autocrypt-level-1-enabling-encryption-avoiding-annoyances.

[17] https://xmpp.org/software.

[18] http://xmpp.org/about/technology-overview.html.

[19] https://otr.cypherpunks.ca/software.php.

[20] The latest version of OTR (v4) aims at supporting asynchronous messaging and out-of-order delivery.

[21] https://whispersystems.org/blog/facebook-messenger.

[22] https://xmpp.org/extensions/xep-0384.html#top.

[23] http://mixminion.net.

[24] https://github.com/cjdelisle/cjdns/blob/master/doc/Whitepaper.md.

[25] 'Alice and Bob' are fictional characters used as placeholder names in cryptology and other computer science/engineering literature to lay out a scenario where there are several participants in a thought experiment or a model.

[26] The Apple vs FBI dispute was a landmark controversy about whether courts can compel communication technology manufacturers to assist in unlocking phones whose data are encrypted. The controversy was spurred by orders issued by US District Courts to Apple in 2015 and 2016.

GLOSSARY

Build: In software development, the term may refer either to the process by which source code is converted into a stand-alone form that can be run on a computer, or to the form itself. One of the most important steps of a software build is the compilation process, where source code files are converted into executable code. See also https://www.techopedia.com/definition/3759/build

Chat-over-email: An approach to designing instant messaging applications using email transfer protocols, such as SMTP and IMAP, often with an implementation of PGP on top, to offer end-to-end encryption. The most well-known projects of a chat-over-email app are Delta Chat, COI, Spike and MailTime.

Client-server: Computer networking model where the machines that communicate are not equivalent: one is a server, permanently on and waiting for connections, the others are clients, who connect when they have something to ask.

Client-side implementation: 'Client-side' means that the action takes place on the user's (the client's) computer, as opposed to 'server-side' which means that the action takes place on a web server.

Constant bit rate encoding: In telecommunications, the term indicates a situation in which the rate at which data is consumed by a codec (a device that encodes or decodes a data stream) is constant.

(Cryptographic) deniability: Encryption technique that allows 'denying' the existence of an encrypted file or message, in the sense that an adversary is unable to prove that the associated data exists.

Double Ratchet: **Key management** algorithm developed by the creators of Signal (Trevor Perrin and Moxie Marlinspike) in 2013, which manages the ongoing renewal and maintenance of short-lived session keys after a first key exchange. It is a 'double' ratchet because it combines a cryptographic component with a key derivation function.

End-to-end encryption: Only the communicating parties can read the message, which is encrypted in transit *and* on users' terminals.

Ephemeral key exchange: See **key exchange**. With ephemeral methods, a different key is used for each connection.

Ephemeral (or disappearing) messaging: Mobile-to-mobile transmission of multimedia messages that automatically disappear from the recipient's screen after the message has been viewed. See also https://searchcio.techtarget.com/definition/ephemeral-messaging

Forking: Forking a piece of software during its development process means that developers take a copy of its source code and start independent development on it, creating a separate piece of software. An act of forking is generally not merely a technical issue, but involves a (governance/organisational) change, possibly conflictual, in the developer community.

Forward/future secrecy: A cryptographic feature of the last generation of instant messaging apps, ensuring that a user's **session keys** will not be compromised even if the private key of the server *is* compromised. In particular, it is meant to protect past sessions against future compromises of secret keys or passwords.

F/OSS (Free and Open-Source Software): Software that anyone is freely licensed to use, copy, study and change in any way, and whose source code is openly shared so that people are encouraged to voluntarily improve the design of the software.

Gossiping/gossip protocol: A process of peer-to-peer communication between computers which ensures that data is disseminated to all members of a group; in the absence of a central registry, the only way to spread data is to rely on each member to pass it along to their neighbours. Thus, gossip protocols are based on the way epidemics spread, and are also called epidemic protocols.

Group messaging: Holding a conversation via a messaging application between two or more people.

Hash: A function that converts an input of letters and numbers into an encrypted output of a fixed length.

Header (email): A code snippet in an HTML email, which precedes the body of the email and contains information about the sender, recipient, the email's route to get to the inbox and a number of authentication details. See https://sendpulse.com/support/glossary/email-header

Interoperability: The ability of programs (messaging apps or any kind of software) to exchange data and communicate smoothly with each other.

IP address: A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address has the two main functions of acting as a host or network interface identifier and providing location addressing.

IPv6: The most recent version of the Internet Protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

Key exchange (v. key discovery): In **public key cryptography**, key exchange is the method by which cryptographic keys are exchanged between two parties; key verification is any way that lets you match a key to a person, making sure that it is indeed that person who uses the key (see e.g. https://ssd.eff.org/en/glossary/key-verification)

Key management: All operations related to the management of cryptographic keys in an encrypted system, including their generation, exchange, storage, use, destruction and replacement.

Latency: In engineering, latency is the time interval between a stimulation and a response, or, from a more general point of view, a time delay between the cause and the effect of some change in the system being observed.

MAC (media access control) address: A unique identifier assigned to a network interface controller (a hardware component connecting a computer to a network) to use as an address in a communication.

Mail User Agent: a computer application that allows a user to send and retrieve email – colloquially called an email program.

Man-in-the-middle attack: In computer security, MITM is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Mesh networks: A network model in which the infrastructure nodes connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data.

Metadata: Succinctly defined as 'information about information', the data providing information about one or more aspects of the data itself. Metadata is used to summarise basic information about data, which can make tracking and working with specific data easier.

Mixnet (mix network): Routing protocols that create hard-to-trace communications by using a chain of servers known as *mixes,* which take in messages from multiple senders, shuffle them and send them back out in random order to the next destination. *De facto*, this breaks the link between the source of the request and the destination, making it harder for third parties to trace end-to-end communications.

Network-layer protection: The network interface layer is the physical interface between the host system and the network hardware, which defines how data packets should be formatted for transmission and routings. This layer has several security vulnerabilities unique to it, needing specific protection responses.

Non-repudiation: Assurance that someone cannot deny the validity of a particular operation; in cryptography, the concept refers to a service that is able to provide proof of the origin of data as well as their integrity.

OMEMO: stands for 'OMEMO Multi-End Message and Object Encryption', an encryption protocol developed to solve specific limitations and problems that existed both in OpenPGP and in OTR. It provides future and forward secrecy and deniability and gives the possibility of message synchronisation and offline delivery.

Open standards and protocols: non-proprietary, open source, well-documented protocols that have been standardised by relevant institutions and are available to be reused and shared by the wider developer community. Open standards are usually believed to ensure better **interoperability** and improve further collaboration between projects based on open standards.

Out of band (data): The data transferred through a stream that is independent from the main data stream ('in band'). An out-of-band data mechanism provides a conceptually independent channel, which allows any data sent via that mechanism to be kept separate from in-band data.

OTR (Off-the-Record Messaging): A cryptographic protocol that provides encryption for instant messaging conversations. In addition to authentication and encryption, OTR provides **forward secrecy**. Version 4 of the protocol (OTRv4) is currently being designed by a team led by Sofía Celi and reviewed by Nik Unger and Ian Goldberg.

Passive attack: An attack on a network in which the attacker does not – as it cannot – interact with any of the parties involved, thus attempting to break the system solely based upon observed data.

Pastebin: A type of online content hosting service where users can store plain text.

Patent disclosure: A public claim of data about an invention; more generally, any part of a patenting process in which data regarding an invention is disclosed to the public. A patent disclosure is used by individuals such as inventors and attorneys, seeking to prepare a patent application. A patent disclosure provides information on the invention and its originality/uniqueness. See also https://www.upcounsel.com/patent-disclosure.

Peer-to-peer (p2p): Computer networking model where two machines or two humans communicate directly to exchange messages, files, or other data.

Primitive (cryptographic): Well-established, low-level cryptographic algorithms, frequently used as a basis to build cryptographic protocols.

Protocol: Referring to the Internet, this word indicates a set of criteria and procedures that provide the conceptual model of the network of networks, as well as the set of specifications that explain how data should be regrouped into packets, addressed, transmitted, routed and received.

Public-key (or asymmetric) cryptography: Cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys known only to the owner.

Public-key infrastructure: The set of roles, policies and procedures needed to create, manage, distribute and use public-key cryptography.

Pull request: In software development, a pull request is a method of submitting contributions to an open development project, which occurs when a developer (or an expert user) asks for changes committed to an external repository to be considered for inclusion in a project's main repository.

PGP (Pretty Good Privacy): An encryption programme that provides privacy and authentication for online communications. PGP is used for signing, encrypting and decrypting texts, e-mails, files, directories and disk partitions, as well as increasing the security of e-mail communications.

Security vs Usability: A widely discussed hypothesis according to which it is extremely hard to design truly secure communication systems and still keep them user-friendly.

Server Name Indication (SNI): An extension to the Transport Layer Security (TLS) computer networking protocol by which a client indicates which hostname it is attempting to connect to at the start of the handshaking process.

Server-side archives: When an e-mail program uses this option, the mail server archives to the mail server itself, or to another server designated as the archive server. This is opposed to client-based archiving, when the individual workstations process mail file archiving. Mail is archived either to the mail server, a designated server, or to its local workstations.

Server-side encryption: Data is encrypted on the server (of the company providing the messaging services).

Social graph: A graph (representation of a structure) representing social relations between a set of entities, e.g. individuals.

TLS (Transport Layer Security): Cryptographic protocol designed to provide communications security over a computer network. TLS aims primarily to provide data integrity and privacy between two or more communicating computer applications.

Two-factor authentication: In an Internet-based service, this is a method of confirming users' claimed identities by using a combination of *two* among these different factors: (1) something they know, (2) something they have, or (3) something they are.

XMPP: Extensible Messaging and Presence Protocol, originally named Jabber and created by the eponymous community, is a communication protocol based on XML (Extensible Markup Language). Unlike most instant messaging protocols, XMPP is defined in an open standard and uses an open systems approach for its development and application. https://xmpp.org/

UI/UX design: User experience design is the process of influencing user behaviour by acting upon some features of a product, such as usability and accessibility. User interface design is the design of the graphical layout of an application – all the items the user interacts with. The two processes are generally considered as part of a whole.

Untrusted server problem: Being able to provide security even in the event of a 'worst case scenario' server breach, where an attacker has full control of server resources, including the ability to read and modify back-end application code and data and remain undetected for at least some time.

Upcycling (of protocols): An approach to designing instant messaging applications by reusing existing open standards and protocols, instead of creating new ones. This approach is said to increase interoperability and help engage bigger communities of developers, as it is based on open standards or well documented protocols.

Usable security: The interdisciplinary research field that addresses the usability of secure communication technologies.

MATTERING PRESS TITLES

Engineering the Climate: Science, Politics and Visions of Control
JULIA SCHUBERT

With Microbes
EDITED BY CHARLOTTE BRIVES, MATTHÄUS REST AND SALLA SARIOLA

Environmental Alterities
EDITED BY CRISTÓBAL BONELLI AND ANTONIA WALFORD

Sensing In/Security
EDITED BY NINA KLIMBURG-WITJES, NIKOLAUS POECHHACKER & GEOFFREY C. BOWKER

Energy Worlds in Experiment
EDITED BY JAMES MAGUIRE, LAURA WATTS AND BRITT ROSS WINTHEREIK

Boxes: A Field Guide
EDITED BY SUSANNE BAUER, MARTINA SCHLÜNDER AND MARIA RENTETZI

An Anthropology of Common Ground: Awkward Encounters in Heritage Work
NATHALIA SOFIE BRICHET

Ghost-Managed Medicine: Big Pharma's Invisible Hands
SERGIO SISMONDO

Inventing the Social
EDITED BY NOORTJE MARRES, MICHAEL GUGGENHEIM, ALEX WILKIE

Energy Babble
ANDY BOUCHER, BILL GAVER, TOBIE KERRIDGE, MIKE MICHAEL, LILIANA OVALLE, MATTHEW PLUMMER-FERNANDEZ AND ALEX WILKIE

The Ethnographic Case
EDITED BY EMILY YATES-DOERR AND CHRISTINE LABUSKI

On Curiosity: The Art of Market Seduction
FRANCK COCHOY

Practising Comparison: Logics, Relations, Collaborations
EDITED BY JOE DEVILLE, MICHAEL GUGGENHEIM AND ZUZANA HRDLIČKOVÁ

Modes of Knowing: Resources from the Baroque
EDITED BY JOHN LAW AND EVELYN RUPPERT

Imagining Classrooms: Stories of Children, Teaching and Ethnography
VICKI MACKNIGHT