

OBJECT LESSONS

BOOK PROPOSAL FORM

NAME: Martin Paul Eve

DATE: January 2015

1. The Book

Title

What specific object do you want to write about?

Password

Summary

Please supply a one-line description of the book summing up its scope and lessons.

The ubiquitous password is the usually accepted standard for identity in the digital era. This book traces its history, development and potential futures as well as the stakes that depend upon this.

Description

Please provide a concise description of the book, outlining your rationale, approach, main themes and style. (250 words)

This book provides a cultural history and analysis of the “password” in both its analogue and digital forms. As the *de facto* standard, in various guises, for remote identification of individuals, the significance of the password as an object cannot be overstated. Yet, to-date, there is virtually no material that treats the password as anything other than a technological phenomenon to be pragmatically implemented or defeated.

To remedy this problematic situation, this book traces the history of the password back to ancient Rome and the “watchwords” of military encampments, through cultural representations (from *Ali Baba* to *Harry Potter*) and up to contemporary implementations in the digital environment. The fundamental historical shift that I argue for in this volume is that passwords have evolved from a meaning of shared knowledge to an equation with identity. Where once passwords denoted identity by the proxy of common knowledge, they are now treated as representative of the individual. In this way, the previously incomprehensible formulation of “identity theft” becomes possible.

Stylistically, the book moves between historical, cultural, philosophical and technological analysis. This must involve, at times, technical and philosophical explanations. In the interests of concision and out of consideration for a diverse audience, though, I will attempt to steer as far away from jargon as possible and, when necessary, will explain technological phenomena in accurate lay terms.

Short non-technical description

Please provide a short description that could be used as the basis for catalogue or jacket copy. This should be clear, informative and persuasive. (150 words or less)

Passwords are crucial to our lives. They regulate our finances, protect our communications and prove who we are to others. They are powerful words. But from where did this equation of verbal knowledge with a person's identity emerge? What does it really mean, in the world of passwords, to say that one's "identity has been stolen"? What does the future of the password hold in store?

In this book Dr. Martin Paul Eve traces the cultural histories of the password from ancient Rome through to biometrics via "open sesame". Equally at ease with cultural analyses of identity as with technological hashing algorithms, this wide-ranging but tightly-focused volume makes a timely and important contribution to an understanding of the words, phrases and special characters that determine where we may enter and even who we are.

Sales features

If you had to give three hooks that will make your book a totally unique approach to the object in question, and that will persuade readers to buy your book, what would they be? (These points should be jargon-free and persuasive.)

1. Passwords are among the most important phrases in modern life but are rarely considered as anything other than contemporary digital inconveniences. This book shows that they have cultural ramifications and histories well beyond this limited scope.
2. We are now used to hearing of "identity theft". What does this phrase actually mean though? *Password* demonstrates that such terminology is only comprehensible in a specific culture of contemporary identity. No longer is your password known, we are told, it is your identity that is stolen. This is a book about how "what you know" became "who you are".
3. Almost everyone knows that they should create a "strong password" for every digital service they use. Far fewer are aware of the rationales for, methods of and challenges in password cracking. This book also traces the parallel counter-histories of those who have sought to undermine systems of identification based upon shared knowledge.

Table of Contents

If applicable, proposed chapter/section titles plus brief descriptions. (Object Lessons books are roughly 25,000 words; you might illustrate here how you plan to cover your topic in this amount of words.)

1: Introduction

3,500 words

This chapter sets the scene for the book by rhetorically questioning the conditions under which passwords emerge and the assumptions that underlie such thinking. I also here briefly lay out the philosophy of quasi-objects (via Latour and Serres) that constitute the object-orientated approach of the volume. Finally, this chapter gives a synopsis of the book's structure as an orientation device for the reader.

2: "Who goes there?": Military, Mortality and Passwords

5,000 words

The second chapter of this book is devoted to military, mortality and passwords. This spans a broad time period, from ancient Egypt through to Gary McKinnon's hacking of the US military via the Enigma machine. It is a worthwhile place from which to begin because military secrets have been among the most tightly protected in human history, for good reason. Indeed, in Max Weber's well-known definition, the state is an entity that "has been successful in seeking to monopolize the legitimate use of physical force within a given territory".¹ Of course, such a definition is overly broad and probably seems naïve in its purported conflation of popular morality with the state. Furthermore, in contemporary cultures of outsourcing and global "black sites", this might be modified to note that a state is now an entity that has been successful in seeking to monopolize the legitimate ability to *authorize others* to use physical force. In any case, though, access to physical force, militarism and violence must be restricted because they threaten human life. Whether this is seen in the economic terms traditionally ascribed as motivations for the state – the creation of a "live, active, productive man" – or because human life is irreplaceable (as either a humanistic or economic sentiment), passwords have often been used as the mechanisms to validate hierarchies and determine access to technologies of death.²

¹Max Weber, *From Max Weber: Essays in Sociology*, ed. & trans. by H.H. Gerth and C. Wright Mills (New York: Oxford University Press, 1946), p. 83

<<https://archive.org/details/frommaxweberessa00webe>> [accessed 10 January 2015].

²Michel Foucault, 'Pastoral Power and Political Reason', in *Religion and Culture*, ed. by Jeremy R. Carrette (Manchester: Manchester University Press, 1999), pp. 135–52 (p. 149).

This chapter begins with an analysis of the reasons why militaries deploy passwords. Although I note that Minoan and, potentially, Minoan, civilizations were non-militaristic (which does not mean that they did not use passwords for civil purposes), I argue that most cultures with militaries have made use of passwords to verify identity. This leads, after a discussion of the two different genealogical etymologies of *arcana* vs. *secretum*, to the various systems described by Aeneas Tacitus for siege defence in the Roman period. Arguing for an analogy between security by obscurity and *arcana* and security by design and *secretum*, I then move towards the use of passwords in cryptography and stenography up to the present day.

3: Special Characters: Passwords in Literature and Film

5,000 words

This third chapter looks at various cultural representations of passwords, when the term is taken in a more lateral way. From ancient Assyrian works of divination, in which it is presumed that the secret knowledge will grant special access to another supernatural realm, through to contemporary fiction and film, the main contention of this chapter is that magic is one of the most common ways in which “passwords” are depicted in cultural works. In fact, the esoteric nature of magic can be said to map exactly on to the intrinsically exclusionary nature of passwords. If everyone could perform magic, it would not, after all, be magic. Magic requires, though, both that the magician *know* the passwords but also that he or she *be* someone with the innate ability to perform the spells. In this way, magic paves the way for an understanding of passwords as words of power and as words that are somehow innately coupled with our identities.

The main cultural works that I examine here are fictional representations of magical passwords. While I will segue from the military context by focusing upon the opening of *Hamlet*, where Francisco demands that Bernardo “unfold” himself, the remainder of the cultural examples here will take the form of magical incantations. For instance, from the moment that Ali Baba overhears the magical phrase of the forty thieves – “open sesame” – notions of secrecy and passwords are central to the well-known tale and its supernatural elements. Likewise, in more contemporary writing and film, the Harry Potter septuplet is emblematic of pre-shared secrets uniting to give access to a hidden realm, be this in the more conventional passwords that grant students access to their common rooms or in the three-factor authentication of ability, wand and magic “password” (incantation) that allow the bearer to perform a spell. In this way, as with the previous chapter on military passwords, I will here show that passwords,

even in their fictional magical forms, are usually used to validate access to spatial, epistemic and practic realms.

4: Passwords and the Digital Era

6,000 words

In the fourth chapter, I trace the evolution of passwords in the era of digital computers. Beginning with time-sharing operating systems such as CTSS (the compatible time-sharing system) this chapter moves through the evolution of the internet, hashing algorithms, asymmetric cryptography and biometrics. This progression towards ever more secure mechanisms for verifying identity brings with it philosophical considerations for how we perceive our selves. For instance, in previous ages, both sides knew the password and an identification was made when a matching phrase was given. In many contemporary computer systems, for example, only one party might know the password while the other will only know the “hash” of the password. This hash is a one-way “distilled essence” of the password. It is possible to derive the hash from the password but not the password from the hash. Crucially, though, when flaws are discovered in hashing algorithms, it may be possible for multiple passwords to result in the same essence (hash). Given how tightly we tend to couple identity with passwords, this chapter investigates how technologies fall short of capturing unique human essences and why, in reality, this is the logical extension, implication and goal of passwords.

The material covered in this chapter is a mixture of technological history and description, given the contemporary importance and relevance of digital passwords, but also the philosophical implications of these technologies. It also begins to tie up work from preceding chapters on spatial distance, the different realms in which passwords are used to secure access, and the future of password technologies. The closing remarks in this chapter open a space for the final discussion of identity that follows in chapter five.

6: Identity

4,000 words

Finally before the conclusion, the fifth chapter binds together the various narratives of identity and passwords that have been woven throughout this book. Examining twenty-first-century rhetorics of transparency, accountability and blame, I will here argue that proxies for identity are at risk of becoming naturalised, as though they were the thing itself. Taking on such terms as “identity theft”, “identity fraud” and “impersonation”, this chapter will examine the implications of the rapidly changing status of passwords for our notions of who we are.

7: Conclusion

1,500 words

Illustrations

Do you need to include any in the book, and if so how many and of what type (e.g. line drawings, diagrams, black & white or color photos). Please note that all illustrations must be supplied as high-resolution files (at least 300 DPI and at least 1000x1000 pixels) and that if your manuscript is accepted for publication, permissions must be cleared by the author or volume editor before production can begin.

No illustrations, although there may be typographical layouts that must be preserved, such as line and column wrapping in the demonstration of a transposition cipher.

Projected completion date

When would you expect the final complete draft of the book to be ready?

Three months after acceptance (earliest: May 2015).

Fit with Object Lessons

Briefly explain why your book project fits with this series. How will your book address your subject 'as an object'? How does your approach differ from traditional cultural studies non-fiction, science and technology journalism, etc.?

As among the most common, but overlooked, objects that we use to validate our identities, a book on passwords would fit well with the Object Lessons series. As historical phenomena that have changed over time, there is a tendency to believe that passwords are a natural, timeless and obvious solution to the problem of identity verification. In one sense, then, this book is an attempt to remove the mask of universality from the password and to show that, in various contexts, passwords have been thought about differently with respect to identity than in our current epoch.

In technical, philosophical terms, this book takes its quasi-object-orientated stance from the work of Bruno Latour and Michel Serres. In this view, passwords are social constructions but they are also, at least partially, agents that condition behaviour. In other words, the idea of a password is a human-made construct. Once it is built, though, it feeds back into notions of naturalization and absolutism.

2. Market and Competition

Market and Readership

How will your proposed Object Lessons book appeal to multiple markets and audiences?

This book has broad appeal to a range of educated readers. There is an increasing interest in cultural, digital histories and this book fits within such emerging paradigms. At the same time, there is no book, as yet, that provides such critical and historical material on passwords. The majority of books on the topic of passwords do not cover this. Instead, such works are usually concerned with pragmatic guidance for programmers on implementing or defeating software-based authentication mechanisms.

As such, this book will appeal to a range of academic readers as well as to a broader public upon whose lives passwords encroach. The diversity of approaches taken here, including military, literary and technological analyses, should ensure that those researching and teaching the disciplines of history, literature, cultural studies and critical technology studies should find this book of interest. Furthermore, with the increasing range of (diverse and often nebulously defined) digital humanities programmes emerging, this book would find a home in a large number of academic courses worldwide, particularly in the Anglophone academy.

Your analysis of competing or comparable books

If applicable, please provide an annotated list of books that are comparable or would compete directly for a reader's attention. Provide the title, author, publisher, publication date and price and explain how your book is like, or unlike, the other books.

There is no book that directly treats this subject or provides direct competition. That said, there have been a number of works published in recent years that form the context for this book's reception. I here provide a representative, but far from comprehensive, selection of such volumes.

Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (Verso, 2014, £16.99)

This book details the exploits (in more than one sense) of the digital hacker collective, "Anonymous". This book has a very different anthropological methodology but it sets the context for an investigation into the "password" and its place among contemporary information security practices. My book works to contextualise the background on passwords, on which works like this focus, within wider notions of identity.

Michael Sean Mahoney, *Histories of Computing*, ed. by Thomas Haigh (Harvard UP, 2011, \$52.50)

As an illustration of the desire for histories of computing and the prominence these are now awarded, there are few better examples of the bridge between academic historians and computer scientists than this collection of Mahoney's work. This book is, obviously, far broader than the specific book on passwords that I am proposing. Once more, though, it sets the scene for critical thinking about technologies that we primarily associate with digital environments.

Karl de Leeuw and Jan Bergstra (eds), *The History of Information Security* (Elsevier, 2007, \$275)

This book is at once the best available resource on the history of information security while also being targeted at a completely different demographic to *Password*. Indeed, the prohibitive price here and far more comprehensive scope will mean that there is very little overlap in terms of market competition. On the other hand, many of the more historical chapters in this book form touchstones for my work. Of particular interest is Edward Higgs's chapter, "From Frankpledge to Chip and Pin: Identification and Identity in England, 1475-2005".

Nick Montfort, Patsy Baudoin, John Bell, Ian Bogost et al., 10 Print CHR#(205.5+RND(1)); : *Goto 10* (MIT Press, 2014, £13.95)

This work, although not pertaining to passwords and therefore clearly not a direct competitor volume, in many ways demonstrates the types of cultural extrapolation that *Password* seeks to make in its own context. While not pushing this as far as in this book – which conceptually weds its production and writing to the topics under discussion – this important work once more contributes to the background within which this work on passwords will be received.

3. Author and contributor information

Your details (title, name and affiliation/job title)

Dr. Martin Paul Eve

Senior Lecturer in Literature, Technology and Publishing
Birkbeck College, University of London
(from May 2015)

Contact information (email, phone, postal address, website, blog, Twitter)

e: martin@martineve.com

t: +44 7985235572

w: <https://www.martineve.com>

HOME ADDRESS

tw: @martin_eve

Suggested Reviewers

Please provide the names of three or four people who are well placed to appraise the merits of your proposed book.

LIST OF REVIEWERS

Previous publications (Does not have to be comprehensive)

Single-authored books:

Open Access and the Humanities: Contexts, Controversies and the Future (Cambridge: Cambridge University Press, 2014)

Pynchon and Philosophy: Wittgenstein, Foucault and Adorno (Palgrave, 2014)

A full list of my journal articles and book chapters can be found at

<http://www.martineve.com/c-v/>

4. Writing sample / imaginary introduction

Please provide a brief sample of writing (under 1000 words) that conveys a sense of the style of the book. You might just riff on one aspect of your object, or you might imagine how the book's introduction would begin.

Please see attached introductory document.

Please return to Ian Bogost at ian.bogost@lmc.gatech.edu or Christopher Schaberg at schaberg@loyno.edu

Thank you!