



# **OBFUSCATION**

## **A USER'S GUIDE FOR PRIVACY AND PROTEST**

**Finn Brunton | Helen Nissenbaum**

The MIT Press  
Cambridge, Massachusetts  
London, England

# CONTENTS

Acknowledgments ix

Introduction 1

## I AN OBFUSCATION VOCABULARY

### 1 Core Cases 8

- 1.1 Chaff: defeating military radar 8
- 1.2 Twitter bots: filling a channel with noise 9
- 1.3 CacheCloak: location services without location tracking 12
- 1.4 TrackMeNot: blending genuine and artificial search queries 13
- 1.5 Uploads to leak sites: burying significant files 14
- 1.6 False tells: making patterns to trick a trained observer 15
- 1.7 Group identity: many people under one name 15
- 1.8 Identical confederates and objects: many people in one outfit 16
- 1.9 Excessive documentation: making analysis inefficient 17
- 1.10 Shuffling SIM cards: rendering mobile targeting uncertain 18
- 1.11 Tor relays: requests on behalf of others that conceal personal traffic 19
- 1.12 Babble tapes: hiding speech in speech 21
- 1.13 Operation Vula: obfuscation in the struggle against Apartheid 21

### 2 Other Examples 25

- 2.1 Orb-weaving spiders: obfuscating animals 25
- 2.2 False orders: using obfuscation to attack rival businesses 25
- 2.3 French decoy radar emplacements: defeating radar detectors 26

- 2.4 AdNauseam: clicking all the ads 26
- 2.5 Quote stuffing: confusing algorithmic trading strategies 27
- 2.6 Swapping loyalty cards to interfere with analysis of shopping patterns 28
- 2.7 BitTorrent Hydra: using fake requests to deter collection of addresses 29
- 2.8 Deliberately vague language: obfuscating agency 30
- 2.9 Obfuscation of anonymous text: stopping stylometric analysis 31
- 2.10 Code obfuscation: baffling humans but not machines 33
- 2.11 Personal disinformation: strategies for individual disappearance 35
- 2.12 Apple's "cloning service" patent: polluting electronic profiling 36
- 2.13 Vortex: cookie obfuscation as game and marketplace 37
- 2.14 "Bayesian flooding" and "unselling" the value of online identity 38
- 2.15 FaceCloak: concealing the work of concealment 39
- 2.16 Obfuscated likefarming: concealing indications of manipulation 40
- 2.17 URME surveillance: "identity prosthetics" expressing protest 40
- 2.18 Manufacturing conflicting evidence: confounding investigation 41

## **II UNDERSTANDING OBFUSCATION**

### **3 Why Is Obfuscation Necessary? 45**

- 3.1 Obfuscation in brief 45
- 3.2 Understanding information asymmetry: knowledge and power 48
- 3.3 The fantasy of opting out 53
- 3.4 Weapons of the weak: what obfuscation can do 55
- 3.5 Distinguishing obfuscation from strong privacy systems 58

### **4 Is Obfuscation Justified? 63**

- 4.1 Ethics of obfuscation 64
- 4.2 From ethics to politics 70

## **5 Will Obfuscation Work? 84**

**5.1 Obfuscation is about goals 85**

**5.2 I want to use obfuscation ... 87**

... to buy some time 88

... to provide cover 88

... for deniability 89

... to prevent individual exposure 89

... to interfere with profiling 90

... to express protest 90

**5.3 Is my obfuscation project ... 90**

... individual, or collective? 91

... known, or unknown? 92

... selective, or general? 92

... short-term, or long-term? 94

**Epilogue 97**

**Notes 99**

**Bibliography 113**

**Index 121**