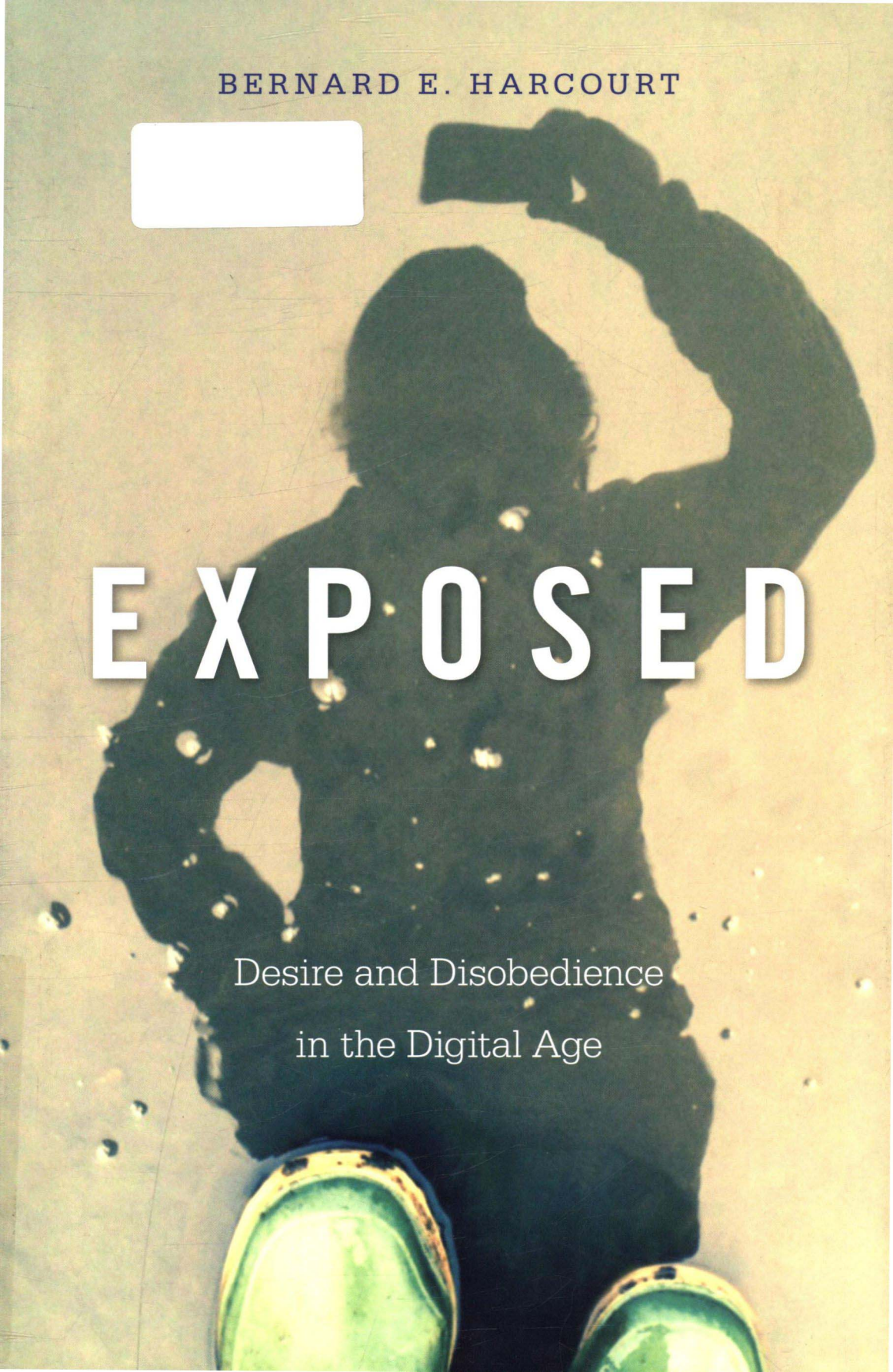
BERNARD E. HARCOURT



EXPOSED

Desire and Disobedience in the Digital Age

"Harcourt's book, which exposes the deeply troubling implications of pervasive surveillance in an era of neoliberalism, could not be more urgent. The developed world is about to make myriad fateful decisions about the degree to which corporate and government leaders monitor us and utilize our data. I can think of no other book I'd rather have leaders consider, as they make these decisions, than Harcourt's."

—FRANK PASQUALE, University of Maryland

"An impassioned plea to liberal democrats to wake up to the perils posed by the new digital technologies to their freedoms and selves. We have become a 'society of expositors,' willingly and naively exposing our most intimate lives to the scrutiny of impersonal agencies, endangering not only our civil liberties but our identities as well."

—SEYLA BENHABIB, Yale University

"This compelling study reveals a radically new form of power to which we freely expose ourselves in a world in which state, economy, and society are no longer separate spheres. Harcourt's vision of this new digital age stands out for its sweep, its vividness, and its analytical precision."

—STEVEN LUKES, New York University

ISBN: 978-0-674-50457-8
90000
9 780674 504578

HARCOURT

EXPOSED

Harvard

EXPOSED

DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE

Bernard E. Harcourt

藏书章

HARVARD UNIVERSITY PRESS

CAMBRIDGE, MASSACHUSETTS

LONDON, ENGLAND

2015

Copyright © 2015 by the President and Fellows of Harvard College
All rights reserved
Printed in the United States of America

First printing

Library of Congress Cataloging-in-Publication Data

Harcourt, Bernard E., 1963–
Exposed : desire and disobedience in the digital age /
Bernard E. Harcourt.
pages cm
ISBN 978-0-674-50457-8 (cloth)
1. Information technology—Social aspects. 2. Privacy,
right of. I. Title.
HM851.H3664 2015
303.48'33—dc23 2015012788

试读结束，需要全本PDF请购买 www.ertongbook.com

EXPOSED

To Isadora

To Léonard

To Mia

EXPOSED

试读结束，需要全本PDF请购买 www.ertongbook.com

CONTENTS

THE EXPOSITORY SOCIETY

EVERY KEYSTROKE, EACH MOUSE CLICK, every touch of the screen, card swipe, Google search, Amazon purchase, Instagram, "like," tweet, scan—in short, everything we do in our new digital age can be recorded, stored, and monitored. Every routine act on our iPads and tablets, on our laptops, notebooks, and Kindles, office PCs and smartphones, every transaction with our debit card, gym pass, E-ZPass, bus pass, and loyalty cards can be archived, data-mined, and traced back to us. Linked together or analyzed separately, these data points constitute a new virtual identity, a digital self that is now more tangible, authoritative, and demonstrable, more fixed and provable than our analog selves. Our mobile phones communicate and search for Wi-Fi networks even when cellular data is turned off. Our MetroCards and employee IDs leave traces with each swipe and tap. Every ATM withdrawal, web search, secured-building entry or elevator ride, every mobile payment leaves a mark that makes it possible for others to know our whereabouts at every moment, to track us at will, and to reconstitute our every action. In sum, today every single digital trace can be identified, stored, and aggregated to constitute a composite sketch of what we like, whom we love, what we read, how we vote, and where we protest.

The social media and web browsers we use—or accidentally visit—constantly collect a trove of our personal data. Our telecommunication

companies record everything they can, as do other telecoms that, unbeknownst to us, route, switch, redirect, and retransmit our communications. Our intimate data are stockpiled by signals intelligence services in the United States and abroad, and by local law enforcement—but also by the retailers we use, by data brokers we've never heard of, by hackers, and simply by the curious among us using free network sniffers or stalking us on the web. Most of our digital information is available one way or another—for purchase by advertisers or for review by insurance companies, for supervision by our employers, for examination by the security apparatus, for capture by keystroke loggers, or for a quick peek on anonymous online message boards. Google and Facebook aggressively compete over who has more of our sensitive data to share with their users and to sell to advertisers. Free off-the-shelf sniffing programs allow anyone to read others' emails and see their web browsing on unsecured networks. Law enforcement agencies secretly collect, pool, and share as much of our digital information as possible. And the National Security Agency (NSA), the British Government Communications Headquarters, the French Direction Générale de la Sécurité Extérieure, the Chinese and Russian signals intelligence agencies, and practically every other intelligence service around the world share the ambition to know everything, to map the Internet universe, to be able to identify every end device connected to the Internet—in short, to know everything digital, everywhere, and at every moment.

Most of us are aware of this, although many of us put it out of our minds. We have read the *Guardian* articles and the *New York Times* and heard the investigative journalism on the radio. We have watched video clips of the congressional hearings. We've repeatedly seen the telltale advertisements popping up on the ribbon of our search screen, reminding us of our immediately past Google or Bing query. We've received the betraying emails in our spam folders. We've even scrutinized the top-secret NSA PowerPoint slides and other documents leaked by Edward Snowden. But it is one thing to know, and quite another to remember long enough to care—especially when there is the ping of a new text, the flag desktop notification of a new email, the

flash of a new like on our Instagram photo, the doorbell noise of a new Facebook message, or just the simple desire to know how many people have seen our Snapchat story or commented on our blog post. It is quite another thing to pay attention in the face of the stimulating distractions and sensual pleasures of the new digital age—the constant news feeds and friend messages, the newest Vine or viral YouTube video, the access to every bit of information online, the ability to Google anything and everything. The anticipation, the desire for something new and satisfying, that sensation we get when we receive a bit of good news in our email in-box—how easily this distracts us from what we actually know about the breathtaking scope and ubiquity of these new forms of digital surveillance, data mining, profiling, and monitoring. We so easily get sidetracked by the most minor digital stimulus—and so often go there to avoid the emotional resistance of writer's block or the discomfort of a difficult thought or unpleasant interaction. How quickly, how instinctively we put our thumb on our smartphone, check email, read the Twitter feed, swipe to Facebook. Whatever. We've already put it out of our mind and are consumed with a new Snapchat, a viral wall post, or Assassin's Creed Unity. We ignore what we suspect or even know about being tracked and exposed. We put it out of our minds. But we do so at our peril.

. . .

The *Wall Street Journal* broke the story in May 2011, well before the name Edward Snowden meant anything to anyone.[1] The revelation did not draw much attention, though. It concerned those little icons on most websites—the thumbs-up of Facebook's like button, the little birdie of Twitter's tweet button, the multicolor Google+ widget, those small icons that line and populate websites, YouTube videos, news articles, travel websites, search ribbons, and so on.

It turns out that those little icons allow Facebook, Twitter, or Google to track our Internet browsing on the websites where the icons are placed, regardless of whether we are logged onto those social networks. As long as someone uses those social networks and has been

logged onto them within the past month (and did not *actively* log out), their Internet surfing on *other sites* that carry those icons is tracked and reported back to Facebook, Twitter, or Google. In fact, you don't even need to be a user of social media—you can be tracked back from the other websites even if you *mistakenly* click onto one of those social media sites. And it turns out that those little icons are on lots of websites. Back in 2011, for instance, 33 percent of the top 1,000 most popular websites had the Facebook like button, 25 percent had the Google+ widget, and 20 percent had the Twitter tweet button. The icons are embedded in millions of websites today.[2]

The sequence is simple: logging onto any of those social media—Facebook, Twitter, Google+—will install software on your web browser that remains active even if you turn off your computer or shut down the browser. It only turns off if you affirmatively log out of the social media—if you intentionally click the "log out" button. Once activated, that software will then report back to the social media anytime you are on any other website that carries the little icon, regardless of whether you click or touch the little icon. Just being on a website with those like and tweet buttons embedded in them will allow those social media to track your Internet browsing.

The *Wall Street Journal* noted in passing, "Facebook says it still places a cookie on the computer of anyone who visits the Facebook.com home page, even if the user isn't a member."[3] So one's browsing history may be made available to others, even for those of us who do not have a Facebook account. The article goes on to report: "Until recently, some Facebook widgets also obtained browsing data about Internet users who had never visited Facebook.com, though Facebook wouldn't know their identity. The company says it discontinued that practice, which it described as a 'bug,' earlier this year after it was disclosed by Dutch researcher Arnold Roosendaal of Tilburg University."[4]

To be more exact, this is precisely how the tracking works. According to detailed communications dating from 2011 between reporters for *USA Today* and Facebook executives—Arturo Bejar, Facebook's engineering director, Facebook spokesmen Andrew Noyes and Barry

试读结束，需要全本PDF请购买 www.ertongbook.com