EXPLODING DATA

RECLAIMING OUR CYBER SECURITY IN THE DIGITAL AGE

MICHAEL CHERTOFF

EXPLODING DATA

RECLAIMING OUR CYBER SECURITY IN THE DIGITAL AGE

MICHAEL CHERTOFF

Atlantic Monthly Press
New York

FIRST EDITION

Published simultaneously in Canada
Printed in the United States of America

First Grove Atlantic hardcover edition: July 2018

Library of Congress Cataloging-in-Publication data is available for this title.

ISBN 978-0-8021-2793-8
eISBN 978-0-8021-6578-7

Atlantic Monthly Press
an imprint of Grove Atlantic
154 West 14th Street
New York, NY 10011

Distributed by Publishers Group West

groveatlantic.com

18 19 20 21 10 9 8 7 6 5 4 3 2 1

CONTENTS

INTRODUCTION

BIG DATA IS WATCHING YOU

ON THE MORNING OF SEPTEMBER 11, 2001, while I drove to my Washington, D.C., office as assistant U.S. attorney general in charge of the Department of Justice Criminal Division, my deputy called to tell me that an airplane had crashed into New York City's World Trade Center. Our initial assumption was that a private-plane pilot had lost his way. But within minutes, the TV news reported a second plane had smashed into the twin towers. That's when we realized America was under attack.

Within minutes we were at the FBI Strategic Information and Operation Center, working with the FBI director to piece together who was attacking us and—importantly—how to prevent further strikes. As we began to pull together the facts, we learned a third aircraft had crashed into the Pentagon. A fourth plane, United Flight 77, had also been hijacked and was headed to Washington, D.C. The order was relayed to fighter jets to shoot down the plane; that

became unnecessary after the passengers heroically stormed the cockpit and forced down the jet in Shanksville, Pennsylvania. America was at war.

Over the next hours and days, we pieced together the identities of the hijackers and concluded that al Qaeda was carrying out its declaration of war against America. Shortly after the attacks, President George W. Bush told the attorney general, "Don't let this happen again." That became our mandate.

This war was different from previous conflicts. Our enemies wore no uniforms and flew no flags; they sought to sneak up on us in the guise of ordinary civilians. Their weapons were homemade explosives. They mingled with the flow of travelers. Against this concealed attacker, radar that we relied upon to warn against enemy missiles or bombers was of no use.

How, then, to detect other terrorists and prevent them from carrying out attacks? We quickly concluded the answer lay in collecting large amounts of information about travelers and foreigners, and discerning the connections and behavior that showed links to a terror network. That meant not only reorienting our intelligence agency to focus on detecting the outlines of the terror network, but also obtaining the capability to detect patterns in the vast amounts of data being collected.

This paradigm shift in national security coincided with the expansion of the internet and the growth of commercial enterprises devoted to using data analytics for marketing and credit-scoring purposes. The private sector, infused with the urgency of preventing further attacks, began to develop

new strategies to find the terrorist needle in the haystack. As the same time, the intelligence community expanded our data haystacks, using new or repurposed legal authorities (including the USA PATRIOT Act, which I participated in drafting) to accumulate information about the global flow of money, people, and communications. Over the next several years, as head of the Department of Justice's Criminal Division and later as U.S. secretary of homeland security, I saw the awesome power of expanded data collection and analytics as tools to protect our nation and its people.

Not surprisingly, these new capabilities began to be deployed for other purposes, including commercial objectives. Just as the civilian internet was spawned by a Defense Department research effort, data collection and analytic tools used in counterterrorism were applied for a host of commercial purposes. Because I was witness to a major turning point in the growth of increasingly pervasive surveillance and the revolution in data collection, storage, and analysis—called "big data" by many—I was acutely aware of the power of data collection and analytics to benefit society. I also knew this information-gathering revolution would challenge America's traditional notions and values in the areas of privacy and liberty.

As time has passed, I have been professionally and personally involved in guiding, prompting, using, and worrying about the ever-expanding harvesting of personal data by both governments and, even more so, the private sector. Perhaps more than most, I understand how much data each of us now generates for collection. That can be beneficial. It can also be very dangerous.