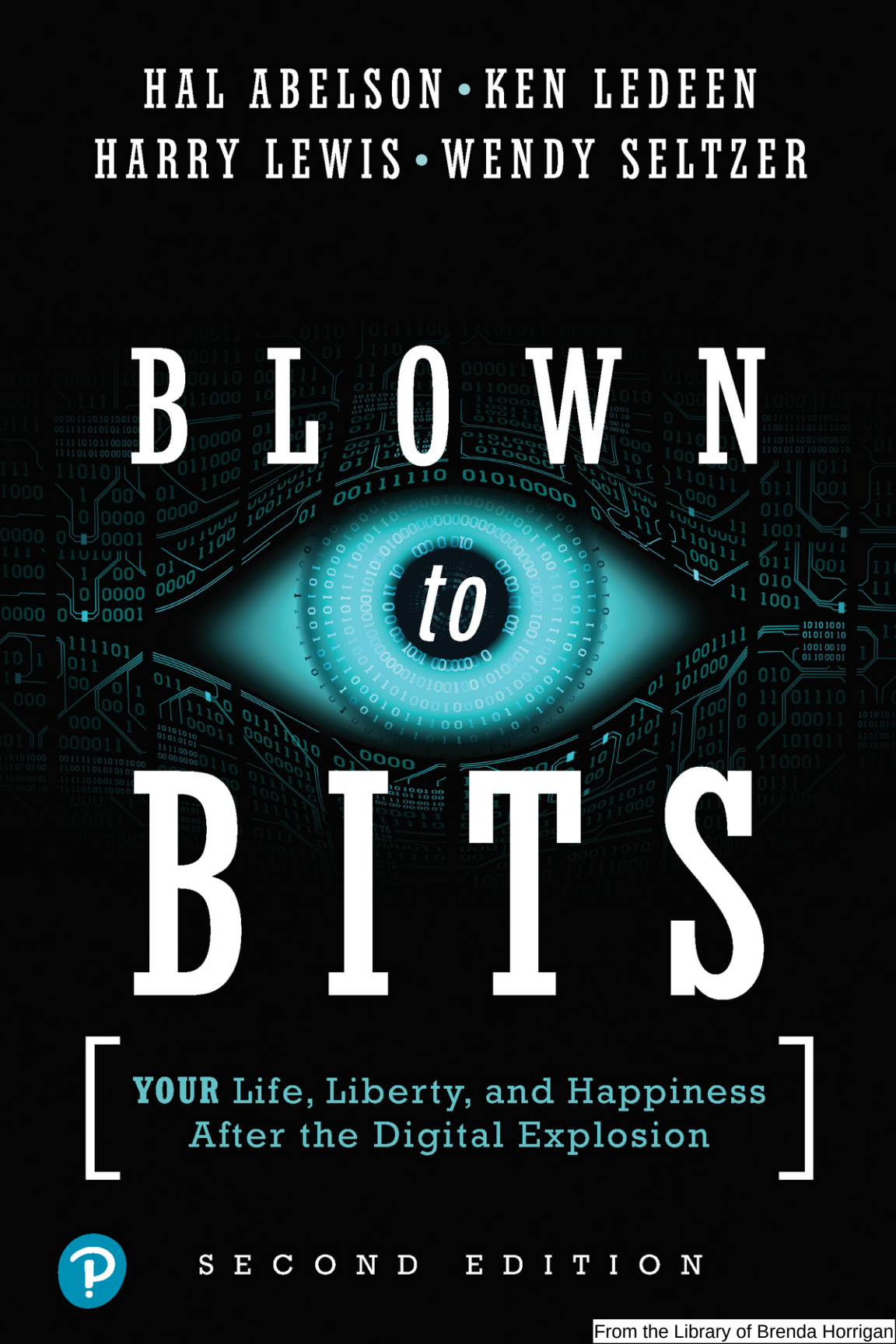
HAL ABELSON • KEN LEDEEN
HARRY LEWIS • WENDY SELTZER

BLOWN to BITS

[YOUR Life, Liberty, and Happiness After the Digital Explosion]



SECOND EDITION

Blown To Bits

Your Life, Liberty, and Happiness After the Digital Explosion

Second Edition

Hal Abelson
Ken Ledeen
Harry Lewis
Wendy Seltzer

Visit us on the web: informit.com/business

Library of Congress Control Number: 2020941961

Published by Pearson Education, Inc.

ISBN-13: 978-0-13-485001-6
ISBN-10: 0-13-485001-7

ScoutAutomatedPrintCode

Editor-in-Chief
Mark L. Taub

Acquisitions Editor
Gregory Doench

Managing Editor
Sandra Schroeder

Senior Project Editor
Lori Lyons

Production Manager
Aswini Kumar/codeMantra

Copy Editor
Kitty Wilson

Indexer
Cheryl Ann Lenser

Proofreader
Abigail Manheim

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

About the Authors

Hal Abelson is Class of 1922 Professor of Computer Science and Engineering at MIT, and an IEEE Fellow. He has helped drive innovative educational technology initiatives such MIT OpenCourseWare, co-founded Creative Commons and Public Knowledge, and was founding director of the Free Software Foundation.

Ken Ledeen, Chairman/CEO of Nevo Technologies, is a serial entrepreneur who has served on the boards of numerous technology companies.

Harry Lewis, former Dean of Harvard College and of Harvard's School of Engineering and Applied Sciences, is Gordon McKay Research Professor of Computer Science at Harvard and Faculty Associate of the Berkman Klein Center for Internet and Society. He is author of *Excellence Without a Soul: Does Liberal Education Have a Future?* and editor of *Ideas that Created the Future: Classic Papers of Computer Science*.

Wendy Seltzer is Counsel and Strategy Lead at the World Wide Web Consortium (W3C), based at MIT. She founded Lumen Database, the pioneering transparency report for online content removals.

CHAPTER 1

Digital Explosion

Why Is It Happening, and What Is at Stake?

This book isn't about computers. It's about your life and mine. It's about how the ground underneath us has shifted in fundamental ways. We all know it is happening. We see it all around us, every day. We all need to understand it more.

The digital explosion is changing everything. In this book we talk about both what is happening and how. We explain the technology itself—why it creates so many surprises and why things often don't work the way we expect them to. It is also about things the information explosion is destroying: old assumptions about our privacy, about our identity, and about who is in control of our lives. It's about how we got this way, what we are losing, and what remains that society still has a chance to put right.

The digital explosion is creating both opportunities and risks. Many of both will be gone in a decade, settled one way or another. Governments, corporations, and other authorities are taking advantage of the chaos, and most of us don't even see it happening. Yet we all have a stake in the outcome. Beyond the science, the history, the law, and the politics, this book is a wake-up call. The forces shaping your future are digital, and you need to understand them.

This book is about the stories we hear and read every day. Stories that are about the profound, often unexpected impact that digital technology is having on our lives. Let's begin with the story of Nicolette Vartuli.

Nicolette couldn't figure out why she didn't get the job. A college senior with a 3.5 GPA, she had prepared for her interview with the investment bank and stayed positive throughout. She kept her head up, smiled, and spoke with confidence. But when the company followed up, it was bad news. She would not be moving on in the hiring process.[1]

Nicolette wanted to know what she had done wrong, but no one could explain why she was rejected—because no one actually knew. She had been interviewed by a computer that used AI software from HireVue to assess her suitability. That software rejected her not because she didn't have some particular qualification but because, as it claimed, the software could detect patterns in people who were successful in the job—and what it observed in Nicolette didn't match. It is easy to understand being rejected because you don't have three years of required experience or some particular skill. This is different. And scary—especially because no explanation was offered for what the software was looking for. And it may be that no explanation could be offered, even if HireVue were willing to disclose its proprietary algorithms. (It is not.)

Companies like this new technology. It is cheaper and more efficient than human interviews. In fact, HireVue, just one of many providers, has completed more than 10 million interviews. Many applicants, by contrast, don't like these automated hiring assistants. It's not just that it feels dehumanizing to be judged by a machine. The companies that offer the service counter that by using technology, more people can get interviews now, and the likelihood of inherent bias on the part of interviewers is diminished. They claim the technology is opening up opportunities, not limiting them—but how do we know?

The instinctive antipathy to automated job screening can't really be because people don't want computers making life-critical decisions. Many such decisions are made by computers today; airplanes and radiation therapy machines are now largely automated systems, for example. Computers now beat highly trained radiologists at spotting cancer tumors in breast X-rays.[2] Would anyone prefer less accurate human screeners? But HireVue's judgments are of a different kind. The program made a decision about Nicolette's humanity. It decided that she was not the sort of person the company should hire, and it did so without explaining to her or anyone else what sort of person would be a good hire and how Nicolette fell short.

Many other systems are today making similar judgments in other human domains. Judges consult computers to assess the risk that criminal defendants will fail to show up for their trials—again by comparing the individuals with others who have been arrested in the past and have been given the benefit of avoiding pretrial detention.[3] Real-estate agents use computers to judge which prospective renters are likely to be deadbeats.[4]

Most of these systems are proprietary, and the companies that make them don't have to disclose how they work. And after all, they argue, human interviewers are no gold standard of impartial judgment. They are prone to all sorts of unfortunate biases and prejudices. That is why tryouts for instrumental musicians are now commonly held out of view of the listeners: When the performers could be seen, women were systematically judged more harshly than men.[5] By matching candidates' interview skills to those of existing workers, HireVue claims, it is

eliminating the most fallible part of the system. It's the human recruiters, HireVue says, who are the "ultimate black box." Maybe—except that HireVue says it is matching candidates to the profile of the best of the bank's current employees. How would anyone know if the software is simply replicating, now automatically, all the prejudices that gave the bank the workforce it now has?

What makes this whole story particularly important is not only that Nicolette was judged by a machine to be unsuitable but that no one—not a human resource manager, not even a programmer—told the HireVue software what criteria to use. It determined those all by itself. The software watched videos of existing employees and picked its own criteria.

The tale of Nicolette's rejected job application is what we call "a bits story." That is, it is not just a job search story; it is a story about the collection, storage, analysis, transmission, and use of trillions of trillions of trillions of individual 0s and 1s. By looking carefully at these stories, we can understand not only the technology behind them, but the implications and risks as well.

Bits represented Nicolette's image as it flowed from her own computer to HireVue's, over wires and cables and probably several kinds of radio waves. The bits were reassembled, taken apart, and analyzed by HireVue's programs. They were somehow compared to trillions of trillions of trillions of bits representing videos of other people, and then a single bit, a single yes or no, came out: continue to the next stage of the hiring process or reject immediately. That bit was a 0 for Nicolette, and that is all she heard back from the company. But HireVue kept all the bits of Nicolette's failed interview; she had to sign over her rights to them in order to get the interview in the first place.

"Algorithmic transparency" is the principle that we should know how computers are making decisions about us. In the words of EPIC (the Electronic Privacy Information Center), "The public has a right to know the data processes that impact their lives so they can correct errors and contest decisions made by algorithms."[6]

New technologies interact in odd ways with evolving standards of privacy, communications practices, and criminal law. Nicolette's story, while important to her, is just one of thousands of bits stories that could be told about any one of us. Every day we encounter unexpected consequences of data flows that could not have happened a few years ago.

When you have finished reading this book, you should see the world in a different way. You should hear a story from a friend or on a newscast and say to yourself, "That's really a bits story," even if no one mentions anything digital. The movements of physical objects and the actions of flesh-and-blood human beings are only the surface. To understand what is really going on, you have to see the virtual world, the eerie flow of bits steering the events of life.

This book is your guide to this new world.

The Explosion of Bits, and Everything Else

The world changed very suddenly. Almost everything is stored in a computer somewhere. Court records, grocery purchases, precious family photos and priceless Hollywood movies, pointless television shows....Computers contain a lot of stuff that isn't useful today but somebody thinks might someday come in handy. It is all being reduced to 0s and 1s—"bits." The bits are stashed on disks of home computers, in the data centers of big corporations and government agencies. Many of the disks aren't even round, spinning things—they are a different kind of storage media, called "disks" for historical reasons. Most of the disks these days are "in the cloud"—just a fancy name for disks owned by a big company such as Amazon and rented out to whoever needs space to store stuff. The disks can hold so many bits that there is no need to pick and choose what gets remembered.

"Bit" is shorthand for "binary digit." The binary number system uses just two digits, 0 and 1, instead of the ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 used in the decimal number system. The first clear statement of the principles of binary notation was given by Gottfried Wilhelm Leibniz in 1679.

So much digital information, misinformation, data, and garbage is being squirreled away that most of it will be seen only by computers, never by human eyes. And computers are getting better and better at extracting meaning from all those bits—finding patterns that sometimes solve crimes, diagnose diseases, and make useful suggestions—and sometimes reveal things about us we did not expect others to know.

The tale of Edward Snowden, who leaked thousands of highly secret government documents in 2013, is a bits story. He brought the documents out of the United States on his laptop; only a few years earlier, he would have needed to carry hundreds of pounds of paper. And everything he disclosed was about government electronic surveillance, raising fundamental questions about trade-offs between privacy and security.

The grounding of the 737 Max in 2019 was not just an airplane story. It was also a bits story. The engines of earlier model 737s had been moved, changing the airplane's weight distribution; software written to process

sensor data and automatically control the airplane's movements did not work as intended.[7]

But it is not just events of global significance that are bits stories; it's the day-to-day stories of ordinary life. The creepy experience of recreational runner Rosie Spinks is a bits story. Spinks used an app on her phone to keep track of her routes and times, and she thought her whereabouts were being kept secret because she had the app's so-called "Enhanced Privacy" setting on. Only when strangers started "liking" her workouts while she was traveling abroad did she realize that "Enhanced Privacy" actually meant "tell random men about my runs if I'm on the leader board." The fitness app was also a social network app, and Rosie's data was being commercialized.[8]

Once something is on a computer, it can replicate and move around the world in a heartbeat. Making a million perfect copies takes but an instant—copies of things we want everyone in the world to see and also copies of things that weren't meant to be copied at all.

The digital explosion is changing the world as much as printing once did—and some of the changes are catching us unaware, blowing to bits our assumptions about the way the world works.

The digital explosion can seem benign, amusing, or even utopian. Instead of sending prints through the mail to Grandma, we share pictures of our children on Instagram. Then not only can Grandma see them but so can Grandma's friends and anyone else. We enjoy the benefits, but what are the risks? The photos are cute and harmless. But suppose a tourist takes a vacation snapshot, and you just happen to appear in the background, at a restaurant where no one knew you were dining. If the tourist uploads his photo and makes it public, the whole world could know where you were and when you were there. Face recognition, which only a few years ago was beyond the capabilities of computers, is now good enough that the tourist photo could even get tagged with your name. It might not happen because a policy or a law prohibits it, but technological limitations won't. Identifying faces in crowds automatically is now a solved problem, and software to do this is being used in China and other authoritarian regimes to discourage public protests and generally to keep track of citizens' whereabouts. And this technology is being used in the United States, too: With the aid of billions of labeled photos gathered from Facebook and other social media, a small company named Clearview AI suddenly became a tool of many law enforcement agencies and even security-conscious private companies.[9] It wasn't even very hard to do—for an entrepreneurial company willing to stretch the limits of the appropriate use

of the massive photographic databases that Facebook and other companies had gathered.

And before we leave the topic of family photos—remember when they were all printed on paper and lasted for decades? Not so anymore. The wondrous benefits of digital images also make them inaccessible. You can't put digital images in a box under your bed for your grandchildren to find. All those family memories may well be lost in the future. There is a good and bad side to pretty much everything in the digital world.

Data leaks. Credit card records are supposed to stay locked up in a data warehouse, but they escape into the hands of identity thieves. And we give information away just because we get something back for doing so. A company will give you free phone calls to anywhere in the world—if you don't mind watching ads for the products its computers hear you talking about. Google will suggest restaurants you might like—if you will leave location tracking on so Google knows what restaurants you already frequent. If you have a meal, Google will ask you if you enjoyed it—no software is yet able to figure *that* out by itself—and into the data maw goes your answer to help Google make recommendations to you and others (and make a little money along the way).

And these are merely some of the things that are happening today. The explosion, and the social disruption it will create, have barely begun.

We already live in a world in which there is enough memory *just in cell phones* to store every word of every book in the Library of Congress billions of times over. Every day, enough video is uploaded to YouTube to record every moment of an entire human lifetime. The explosive growth is still happening. Every year we can store more information, move it more quickly, and do far more ingenious things with it than we could the year before. Now that refrigerators and vacuum cleaners create data, the increasing rate at which data is created is almost unimaginable. Most of the data that has ever existed was created in the past year—and that will be true again next year and the year after that.

So much disk storage is being produced every year that it could be used to record a page of information, every few seconds, about you *and every other human being on earth*. A remark made long ago can come back to haunt a political candidate, and a letter jotted quickly can be a key discovery for a biographer. Imagine what it would mean to record every word every human being speaks or writes in a lifetime. The technological barrier to that has already been removed: There is enough storage to remember it all. YouTube says that 500 hours of video are uploaded every minute.[10] Should any social barrier stand in the way?

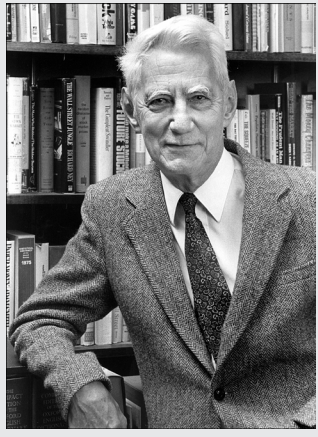
Sometimes things seem to work both better and worse than they used to. A "public record" is now *very* public. Before you get hired in Nashville,

Tennessee, your employer can figure out if you were caught ten years ago taking an illegal left turn in Lubbock, Texas. The old notion of a "sealed court record" is mostly a fantasy in a world where tidbits of information are duplicated, cataloged, and moved around endlessly. In Europe a new "right to be forgotten" has been added to the list of human rights, intended to protect people from having to carry every youthful indiscretion with them forever; but in the United States the right to free speech remains dominant, and the collision between these conflicting rights is inevitable. In the bits world, the Atlantic ocean can be crossed in microseconds.

With hundreds of TV and radio stations and millions of websites, Americans love the variety of news sources, but they have adjusted uncomfortably to the displacement of more authoritative sources. In China, the situation is reversed: The technology creates greater government control of the information its citizens receive, as well as better tools for monitoring their behavior.

The Koans of Bits

Bits behave strangely. They travel almost instantaneously, and they take almost no space to store. We have to use physical metaphors to make them understandable. We liken them to dynamite exploding or water flowing. We even use social metaphors for bits. We talk about two computers agreeing on some bits and about people using burglary tools to steal bits. Getting the right metaphor is important, but so is knowing the limitations of our metaphors. An imperfect metaphor can mislead as much as an apt metaphor can illuminate.



CLAUDE SHANNON

Claude Shannon (1916–2001) is the undisputed founding figure of information and communication theory. While working at Bell Telephone Laboratories after the Second World War, he wrote the seminal paper "A Mathematical Theory of Communication," which foreshadowed much of the subsequent development of digital technologies. Published in 1948, this paper gave birth to the now-universal realization that the bit is the natural unit of information and to the use of the term.

Reused with permission of Nokia Corporation and AT&T Archives. http:www.bell-labs.com/news/2001/february/26/shannon2_lg.jpeg.

We offer seven truths about bits. We call them "koans" because they are paradoxes, like the Zen verbal puzzles that provoke meditation and enlightenment. These koans are oversimplifications and overgeneralizations. They describe a world that is developing but hasn't yet fully emerged. But even today they are truer than we often realize. These themes will echo through our tales of the digital explosion.

Koan 1: It's All Just Bits

Your computer and your smartphone (really just another computer) successfully create the illusion that they contain photographs, letters, songs, and movies. All they really contain is bits—lots of them—patterned in ways you can't see. Your computer was designed to store just bits; all the files and folders and different kinds of data are illusions created by computer programmers. When you send a message containing a photograph, the computers that handle your message as it flows through the Internet have no idea that what they are handling is part text and part graphic. Telephone calls are also just bits, and that has helped create competition: Traditional phone companies, cell phone companies, cable TV companies, and voice over IP (VoIP) service providers can shuffle bits around to each other to complete calls. The Internet was designed to handle just bits, not emails or attachments, which are inventions of software engineers. We couldn't live without those more intuitive concepts, but they are artifices. Underneath, it's all just bits.

This koan is more consequential than you might think. Consider the story of Naral Pro-Choice America and Verizon Wireless. Naral wanted to form a text messaging group to send alerts to its members. Verizon decided not to allow it, citing the "controversial or unsavory" things the messages might contain.[11] Text message alert groups for political candidates it would allow, but not for political causes it deemed controversial. Had Naral simply wanted telephone service or an 800 number, Verizon would have had no choice. Telephone companies were long ago declared "common carriers." Like railroads, phone companies are legally prohibited from picking and choosing customers from among those who want their services. In the bits world, there is no difference between a text message and a wireless phone call. It's all just bits, traveling through the air by radio waves. But the law hasn't caught up to the technology. It doesn't treat all bits the same, and the common carriage rules for voice bits don't apply to text message bits.

Exclusive and Rivalrous

Economists would say that bits, unless controlled somehow, tend to be non-exclusive (once a few people have them, it is hard to keep them from others) and non-rivalrous (when someone gets them from me, I don't have any less). In a letter he wrote about the nature of ideas, Thomas Jefferson eloquently stated both properties: "If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of every one, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it."[12]

Verizon backed down in the case of Naral, but not on the principle. A phone company can do whatever it thinks will maximize its profits in deciding whose messages to distribute. Yet no sensible engineering distinction can be drawn between text messages, phone calls, and any other bits traveling through the digital airwaves.

Koan 2: Perfection Is Normal

To err is human. When books were laboriously transcribed by hand in ancient scriptoria and medieval monasteries, errors crept in with every copy. Computers and networks work differently. Every copy is perfect. If you email a photograph to a friend, the friend won't receive a fuzzier version than the original. The copy will be identical, down to levels of detail too small for the eye to see.

Computers do fail, of course. Networks break down, too. If the power goes out with no battery backup, nothing works at all. So the statement that copies are normally perfect is only relatively true. Digital copies are perfect only to the extent that they can be communicated at all. And yes, it is possible in theory that a single bit of a big message will arrive incorrectly—but it's also possible that a volcano will erupt under you, and you won't get the message at all. The odds of an erroneous bit are lower than the odds of a physical catastrophe, and that is good enough for all practical purposes.

Networks don't just pass bits from one place to another. They check to see if the bits seem to have been damaged in transit and correct them or retransmit them if they seem incorrect. As a result of these error detection and correction mechanisms, the odds of an actual error—a character being wrong in an email, for example—are so low that we would be wiser to worry instead about a meteor hitting our computer, improbable though precision meteor strikes may be.

The phenomenon of perfect copies has drastically changed the law, a story told in Chapter 6, "Balance Toppled." In the days when music was distributed on audio tape, teenagers were not prosecuted for making copies of songs because the copies weren't as good as the originals, and copies of copies would be even worse. The reason that people today more often subscribe to music services than own their own copies of recordings is that copies are perfect—not just as good as the original but identical to the original so that even the notion of "original" is meaningless. The consequences of digital disruption of "intellectual property" are not over yet. Bits are an odd kind of property. Once I release them, everybody has them. And if I give you my bits, I don't have any fewer.

Koan 3: There Is Want in the Midst of Plenty

Vast as worldwide data storage is today, two years from now, it will be twice as large. Yet the information explosion means, paradoxically, the loss of information that is not online. One of us saw a new doctor at a clinic he had been using for decades. She showed him dense charts of his blood chemistry, data transferred from his home medical device to the clinic's computer—more data than any specialist could have had at her disposal five years ago. The doctor then asked whether he had ever had a stress test and what the test had shown. Those records should be all there, the patient explained, in the medical file. But the information was in the *paper* file, to which the doctor did not have access. It wasn't in the *computer's* memory, and the patient's memory was being used as a poor substitute. The old data might as well not have existed at all since it wasn't digital.

Even information that exists in digital form is useless if there are no devices to read it. The rapid progress of storage engineering has meant that data stored on obsolete devices effectively ceases to exist. A twentieth-century digital update of the eleventh-century British *Domesday Book* shown in Figure 1.1 was useless by the time it was only one-sixtieth the age of the original.

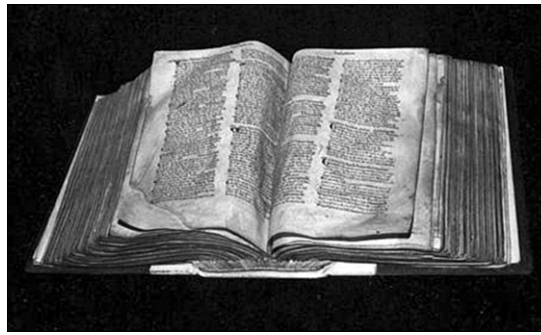


FIGURE 1.1 The Domesday Book of 1086. A 900th anniversary digital update was unreadable 15 years later.[13]

Or consider search, among the subjects of Chapter 4, "Gatekeepers." At first, search engines such as Google were interesting conveniences that a few people used for special purposes. With the growth of the World Wide Web and the explosion of online information, search engines became the first place many people look for information—even before they look in books or ask friends. Appearing prominently in search results has become a matter of life or death for businesses. We may move on to purchase from a competitor if we can't find the site we wanted in the first page or two of results. We may assume something didn't happen if we can't find it quickly in an online news source. If it can't be found—quickly—it's just as though it doesn't exist at all.

And some information isn't true. All of the mechanisms that enable the communication and storage of facts also work for falsehoods. Ugliness and cruelty are as easily captured in bits as beauty and kindness. The market economics of information change when everyone can be a publisher and no one needs an editor. Floods of misinformation, disinformation, and garbage can overwhelm truth and beauty. Authoritarian societies may be able to manage the flow of bits more efficiently than free societies, which risk being undercut by their own principles of information freedom.

Koan 4: Processing Is Power

The speed of a computer is usually measured by the number of basic operations, such as additions, that can be performed in one second. The fastest computers available in the early 1940s could perform about five operations per second. The fastest today can perform about a trillion. Buyers of personal computers know that a machine that seems fast today will seem slow in a year or two.

For at least three decades, the increase in processor speeds was exponential. Computers became twice as fast every couple of years. These increases were one consequence of Moore's Law (see sidebar).

Since 2001, processor speed has not followed Moore's Law; in fact, processors have hardly grown faster at all. But that doesn't mean that computers

Moore's Law

Gordon Moore, founder of Intel Corporation, observed that the density of integrated circuits seemed to double every couple of years. This observation is referred to as "Moore's Law." Of course, it is not a natural law, like the law of gravity. Instead, it is an empirical observation of the progress of engineering and a challenge to engineers to continue their innovation. In 1965, Moore predicted that this exponential growth would continue for quite some time.[14] That it has continued for more than 40 years is one of the great marvels of engineering. No other effort in history has sustained a growth rate anywhere close to this.

won't continue to get faster. New chip designs include multiple processors on the same chip so the work can be split up and performed in parallel. Such design innovations promise to achieve the same effect as continued increases in raw processor speed. And the same technology improvements that make computers faster also make them less expensive.

The rapid increase in processing power means that inventions move out of labs and into consumer goods very quickly. Robot vacuum cleaners and self-parking vehicles were possible in theory a decade ago, but now they have become consumer items. Tasks that today seem to require uniquely human skills are no longer just the subject of research projects in corporate or academic laboratories; they are incorporated in consumer products. Face recognition and voice recognition are here and now; telephones know who is calling, and surveillance cameras don't need humans to watch them. The power comes not just from the bits but from being able to do things with the bits.

Koan 5: More of the Same Can Be a Whole New Thing

The explosive growth is exponential growth—doubling at a steady rate. Imagine earning 100% annual interest on your savings account: In 10 years, your money would have increased more than a thousandfold, and in 20 years, more than a millionfold. A more reasonable interest rate of 5% will hit the same growth points, but it will do so 14 times more slowly. Epidemics initially spread exponentially, as each infected individual infects several others.

When something grows exponentially, for a long time it may seem not to be changing at all. If we don't watch it steadily, it will seem as though something discontinuous and radical occurred while we weren't looking.

That is why epidemics at first go unnoticed, no matter how catastrophic they may be when full-blown. Imagine 1 sick person infecting 2 healthy people, and the next day each of those 2 infects 2 others, and the next day after that each of those 4 infects 2 others, and so on. The number of newly infected each day grows from 2 to 4 to 8. In a week, 128 people come down with the disease in a single day, and twice that number are now sick, but in a population of 10 million, no one notices. Even after two weeks, barely 3 people in a 1,000 are sick. But after another week, 40% of the population is sick, and society collapses. The 2019–2020 coronavirus pandemic followed pretty much this pattern in parts of the world where societies did not react quickly. At the start of the epidemic in Wuhan, the number of cases doubled about every three days.[15]

Exponential growth is actually smooth and steady; it just takes very little time to pass from unnoticeable change to highly visible. Exponential growth of anything can suddenly make the world look utterly different than it had been. When that threshold is passed, changes that are "just" quantitative can look qualitative.

Another way of looking at the apparent abruptness of exponential growth—its explosive force—is to think about how little lead time we have to respond to it. Our hypothetical epidemic took three weeks to overwhelm the population. At what point was it only half as devastating? The answer is *not* "a week and a half." The answer is *on the next-to-last day*. Suppose it took a week to develop and administer a vaccine. Then noticing the epidemic after a week and a half would have left ample time to prevent the disaster. But that would have required understanding that there *was* an epidemic when only 2,000 people out of 10 million were infected.

The information story is full of examples of unperceived changes followed by dislocating explosions. Those with the foresight to notice the explosion just a little earlier than everyone else can reap huge benefits. Those who move a little too slowly may be overwhelmed by the time they try to respond. Take the case of digital photography.

In 1983, Christmas shoppers could buy digital cameras to hook up to their IBM PC and Apple II home computers. The potential was there for anyone to see; it was not hidden in secret corporate laboratories. But digital photography did not take off. Economically and practically, it couldn't. Cameras were too bulky to put in your pocket, and digital memories were too small to hold many images. Even 14 years later, film photography was still a robust industry. In early 1997, Kodak stock hit a record price, with a 22% increase in quarterly profit, "fueled by healthy film and paper sales...[and] its motion picture film business," according to a news report.[16] The company raised its dividend for the first time in eight years. But by 2007, digital memories had become huge, digital processors had become fast and compact, and both were cheap. As a result, cameras had become little computers. The company that was once synonymous with photography was a shadow of its former self. Kodak announced that its employee force would be cut to 30,000, barely a fifth the size it was during the good times of the late 1980s.[17] By 2018, that number was down to about 5,400. Bits took away 90% of the jobs. Moore's Law moved faster than Kodak did.

In the rapidly changing world of bits, it pays to notice even small changes—and to do something about them.

Koan 6: Nothing Goes Away

25,000,000,000,000,000,000.

That is the number of bits that were created and stored every day of 2019, according to one industry estimate. The capacity of disks has followed its own version of Moore's Law, doubling every two or three years. Far more data is created by every manner of device but not stored.

In financial industries, federal laws now *require* massive data retention to assist in audits and investigations of corruption. In many other businesses, economic competitiveness drives companies to save everything they collect and to seek out new data to retain. Tens of millions of transactions occur in Walmart stores every day, and every one of them is saved: date, time, item, store, price, who made the purchase, and how—credit, debit, cash, or gift card. Such data is so valuable to planning the supply chain that stores will pay money to get more of it from their customers. That is really what loyalty programs at supermarkets and other stores provide: Shoppers are supposed to think that the store is granting them a discount in appreciation for their steady business, but actually the store is paying them for information about their buying patterns. We might better think of a privacy tax: We pay the regular price *unless* we want to keep information about our food, alcohol, and pharmaceutical purchases from the market; to keep our habits to ourselves, we pay extra.

The massive databases challenge our expectations about what will happen to the data about us. Take something as simple as a stay in a hotel. When you check in, you are given a keycard, not a mechanical key. In fact, some hotels have gone one step further, having you use your own cell phone as the room key. Because the keycards can be deactivated instantly, there is no longer any great risk associated with losing your key, as long as you report it missing quickly. On the other hand, the hotel now has a record, accurate to the second, of every time you entered your room, used the gym or the business center, or went in the back door after-hours. The same database could identify every cocktail and steak you charged to the room, which other rooms you phoned and when, and the brands of tampons and laxatives you charged at the hotel's gift shop. This data might be merged with billions of bits' worth of other data, analyzed, and transferred to the parent company, which owns restaurants and fitness centers as well as hotels. It might also be lost, or stolen, or subpoenaed in a court case.

The ease of storing information has meant asking for more of it. Birth certificates used to include just the information about the child's and parents' names, birthplaces, and birthdates, plus the parents' occupations. Now the electronic birth record includes how much the mother drank and smoked during her pregnancy, whether she had genital herpes or a variety of other medical conditions, and both parents' Social Security numbers. Opportunities for research are plentiful, and so are opportunities for mischief and catastrophic accidental data loss.

The data will all be kept forever, unless there are policies to get rid of it.

And the data will all be kept forever unless there are policies to get rid of it. For the time being at least, the data sticks around. And because databases are intentionally

duplicated—backed up for security or shared while pursuing useful analyses—it is far from certain that data can ever be permanently expunged, even if we wish that to happen. The Internet consists of millions of interconnected computers; once data gets out, there is no getting it back. Victims of identity theft experience daily the distress of having to remove misinformation from the record. It seems never to go away.

Koan 7: Bits Move Faster Than Thought

The Internet existed before there were personal computers. It predates the fiber-optic communication cables that now hold it together. When it started around 1970, ARPANET, as it was called, was designed to connect a handful of university and military computers. No one imagined a network connecting tens of millions of computers and shipping information around the world in the blink of an eye. (In fact, no one imagined that so many computers would even exist.) Even the engineer who was charged with designing the gateways that would connect the computers together remembers his reaction to the idea of a computer network: "Looks like a straightforward engineering job; we could certainly do it, but I can't imagine why anyone would want such a thing."[18] Along with processing power and storage capacity, networking has experienced its own exponential growth in the number of computers interconnected and the rate at which data can be shipped over long distances, from space to earth and from service providers into private homes.

The Internet has caused drastic shifts in business practice. Customer service calls are outsourced to India today not just because labor costs are low there. Labor costs have *always* been low in India, but international telephone calls used to be expensive. Calls about airline reservations and lingerie returns are answered in India today because it now takes almost no time and costs almost no money to send to India the bits representing your voice. The same principle holds for professional services. When you are X-rayed at your local hospital in Iowa, the radiologist who reads the X-ray may be half a world away. The digital X-ray moves around the world and back faster than a physical X-ray could be moved between floors of a hospital. When you place an order at a drive-through station at a fast food restaurant, the person taking the order may be in another state. She keys the order so it appears on a computer screen in the kitchen, a few feet from your car, and you are none the wiser. Such developments are causing massive changes to the global economy, as industries figure out how to keep their workers in one place and ship their business as bits.

In the bits world, in which messages flow instantaneously, it sometimes seems that distance doesn't matter at all. The consequences can be startling. One of us, while dean of an American college, witnessed the shock of a father

receiving condolences on his daughter's death. The story was sad but familiar, except that this version had a startling twist. Father and daughter were both in Massachusetts, but the condolences arrived from halfway around the world before the father had learned that his daughter had died. News, even the most intimate news, travels fast in the bits world once it gets out.

When everyone is connected all the time, people can organize themselves as never before. Those afflicted with rare diseases or inspired by idiosyncratic interests can stroke a few keys and share their experiences, though they are separated by oceans and will never meet in person. And those united by a common cause can organize to air their grievances, as the digital-savvy youth of Hong Kong did with great skill during the pro-democracy protests of 2014. But in the hands of the authorities, the bits the protesters exchanged became evidence against them. By the time of the 2019 Hong Kong protests, organizers had abandoned Facebook and were resorting to less convenient encrypted texting apps—and were wearing face masks to confuse the government's face surveillance systems.[19]

And if surveillance fails, governments can simply shut down the Internet. That happened in the Muslim-majority Indian state of Kashmir in 2019; there was no Internet for 7 months, in the interest of "public safety."[20] Similar shutdowns happened in 2019 in Iran, Congo, Bangladesh, and more than a dozen other countries.[21] And in the United States, Section 706 of the Communications Act of 1934 authorizes the president to shut down "a facility for wire communication" in case of "a state or threat of war"—a very sweeping authorization, thus far never invoked to gain control of the Internet.

The instantaneous communication of massive amounts of information has created the misimpression that there is a place called "cyberspace," a land without frontiers where all the world's people can be interconnected as though they were residents of the same small town. That concept has been decisively refuted by the actions of the world's courts. National and state borders still count—and count a lot. If a book is bought online in England, the publisher and author are subject to British libel laws rather than those of the homeland of the author or publisher. Under British law, defendants have to prove their innocence; in the United States, plaintiffs have to prove the guilt of the defendants. An ugly downside to the explosion of digital information and its movement around the world is that information may become less available even where it would be legally protected. (We return to this subject in Chapter 7, "You Can't Say That on the Internet.") "Right to be forgotten" laws may require information to disappear—not just in the country where an individual has asked for some past misdeed to be struck from the electronic record but everywhere. Such a law might seem to be unenforceable, but the companies making the information available—Google, for example—operate internationally, and if they violate the law anywhere, they risk having

employees harassed or arrested any time they are within a jurisdiction where the law has been violated or ignored. Similarly, the publishing world has been blown to bits. It used to be possible to publish a bowdlerized edition of a book or an edited edition of a newspaper in countries with strict speech codes, but now the bits can readily flow from less censorious regions to more. It may prove simpler to publish only a single version of a work for sale everywhere, an edition omitting information that might somewhere excite a lawsuit.

Good and Ill, Promise and Peril

The digital explosion has thrown a lot of things up for grabs, and we all have a stake in who does the grabbing. The way the technology is offered to us, the way we use it, and the consequences of the vast dissemination of digital information are matters not in the hands of technology experts alone. Governments and corporations and universities and other social institutions have a say. And ordinary citizens, to whom these institutions are accountable, can influence their decisions. Important choices are made every year, in government offices and legislatures, in town meetings and police stations, in the corporate offices of banks and insurance companies, in the purchasing departments of chain stores and pharmacies. We can all help raise the level of discourse and understanding. We can all help ensure that technical decisions are made in a context of ethical standards.

We offer two basic morals. First, information technology is inherently neither good nor bad; it can be used for good or ill, to free us or to shackle us. Second, new technologies bring social change, and change comes with both risks and opportunities. All of us, and all of our public agencies and private institutions, have a say in whether technology will be used for good or ill and whether we will fall prey to its risks or prosper from the opportunities it creates.

Technology Is Neither Good nor Bad

Any technology can be used for good or ill; digital technologies, in particular, can be simultaneously good and bad. Nuclear reactions create electric power and weapons of mass destruction. These two uses share a common core but are otherwise quite distinct. Not so in the world after the digital explosion.

The same encryption technology that makes it possible for you to email your friends with confidence that no eavesdropper will be able to decipher your message also makes it possible for terrorists to plan their attacks undiscovered. The same Internet technology that facilitates the widespread distribution of educational works to impoverished students in remote locations

also enables massive copyright infringement. The photomanipulation tools that enhance your snapshots are used by child pornographers to escape prosecution.

The same technologies can be used to monitor individuals, to track their behaviors, and to control what information they receive. Search engines need not return unbiased results. Many users of web browsers do not realize that the sites they visit archive their actions. There is probably a record of exactly what you have been accessing and when, as you browse a clothing or book store catalog, a site selling pharmaceuticals, or a service offering advice on contraception or drug overdose. There are vast opportunities to use this information for invasive but relatively benign purposes, such as marketing, and also for more questionable purposes, such as blacklisting and blackmail.

The key to managing the ethical and moral consequences of technology while nourishing economic growth is to *regulate the use* of technology without *banning or restricting its creation*.

Few regulations mandate disclosure that the information is being collected or restrict the use to which the data can be put. The USA PATRIOT Act and other federal laws give government agencies sweeping authority to sift through mostly innocent data looking for signs of "suspicious activity" by potential terrorists—and to notice lesser transgressions in the process. Although the World Wide Web reaches into millions of households, the rules and regulations governing it are not much better than those of a lawless frontier town of the Old West.

New Technologies Bring Both Risks and Opportunities

The same large storage media that enable anyone to analyze millions of baseball statistics also allow anyone with access to confidential information to jeopardize its security. Access to aerial maps via the Internet makes it possible for criminals to plan burglaries of upscale houses, but technologically sophisticated police know that records of such queries can also be used to solve crimes.

Social networking tools such as Facebook and Twitter have made their founders quite wealthy and have given birth to many thousands of new friendships, marriages, and other ventures. But interconnectivity has unexpected side effects, too. A woman in England discovered that her fiancé was married when Facebook suggested his wife as someone she might want as a friend.[22] And in 2019 a Massachusetts college student committed suicide by jumping from the fourth floor of a parking garage, having received some 47,000 text messages, many allegedly abusive, from his girlfriend in the previous two months. She was charged with involuntary manslaughter—the same crime she might have been charged with had she instead struck him with her car while driving and texting.[23] In a nation deeply committed to free expression as a legal right, which Internet evils should be crimes, and which are just wrong?

Vast data networks have made it possible to move work to where the people are, not people to the work. The results are enormous business opportunities for entrepreneurs who take advantage of these technologies and new enterprises around the globe, and also the other side of the coin: jobs lost to outsourcing.

The difference every one of us can make, to our workplace or to another institution, can be to ask a question at the right time about the risks of some new technological innovation—or to point out the possibility of doing something in the near future that a few years ago would have been utterly impossible.

We begin our tour of the digital landscape with a look at our privacy, a social structure that the explosion has left in shambles. While we enjoy the benefits of ubiquitous information, we also sense the loss of the shelter that privacy once gave us. And we don't know what we want to build in its place. The good and ill of technology, and its promise and peril, are all thrown together when information about us is spread everywhere. In the post-privacy world, we stand exposed to the glare of noonday sunlight—and sometimes it feels strangely pleasant.

Endnotes

1 Drew Harwell, "A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job," *Washington Post*, November 6, 2019, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

2 Scott Mayer McKinney et al., "International Evaluation of an AI System for Breast Cancer Screening," *Nature* 577, no. 7788 (January 2020): 89–94, https://doi.org/10.1038/s41586-019-1799-6.

3 Julia Angwin et al., "Machine Bias," ProPublica, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

4 Elizabeth Fernandez, "Will Machine Learning Algorithms Erase the Progress of the Fair Housing Act?" *Forbes*, November 17, 2019, https://www.forbes.com/sites/fernandezelizabeth/2019/11/17/will-machine-learning-algorithms-erase-the-progress-of-the-fair-housing-act/.

5 Claudia Goldin and Cecilia Rouse, "Orchestrating Impartiality: The Impact of 'Blind' Auditions on Female Musicians," *The American Economic Review* 90, no. 4 (September 2000), https://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.90.4.715.

6 "Algorithmic Transparency: End Secret Profiling," Electronic Privacy Information Center, March 1, 2020, https://epic.org/algorithmic-transparency/.

7 Benjamin Zhang, "The Boeing 737 Max Is Likely to Be the Last Version of the Best-Selling Airliner of All Time," *Business Insider*, March 19, 2019, https://www.businessinsider.com/boeing-737-max-design-pushed-to-limit-2019-3.

8 Rosie Spinks, "Confused About How to Use Strava Safely? You Are Not Alone," *Quartz*, January 29, 2018, https://qz.com/1191431/strava-privacy-concerns-here-is-how-to-safely-use-the-app/.

9 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

10 J. Clement, "Hours of Video Uploaded to YouTube Every Minute, 2007–2019," *Statista*, August 9, 2019, https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/.

11 Adam Liptak, "Verizon Blocks Messages of Abortion Rights Group," *The New York Times*, September 27, 2007, https://www.nytimes.com/2007/09/27/us/27verizon.html.

12 "Article 1, Section 8, Clause 8: Thomas Jefferson to Isaac McPherson," in Andrew A. Lipscomb and Albert Ellery Bergh, eds., *The Writings of Thomas Jefferson* (Thomas Jefferson Memorial Association, 1905), http://press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html.

13 Robin McKie and Vanessa Thorpe, "Digital Domesday Book lasts 15 years not 1000," *Guardian Unlimited*, March 3, 2002.

14 G. E. Moore, "Cramming More Components onto Integrated Circuits," *Proceedings of the IEEE* 86, no. 1 (January 1998): 82–85, https://doi.org/10.1109/JPROC.1998.658762.

15 Steven Sanche et al., "High Contagiousness and Rapid Spread of Severe Acute Respiratory Syndrome Coronavirus 2," *Emerging Infectious Diseases* 26, no. 7 (July 2020): 1470–1477, https://dx.doi.org/10.3201/eid2607.200282.

16 "Kodak, GE, Digital Report Strong Quarterly Results," *Atlanta Constitution*, January 17, 1997.

17 Claudia H. Deutsch, "Shrinking Pains at Kodak," *The New York Times*, February 9, 2007.

18 Harry R. Lewis, "A Science Is Born," *Harvard Magazine*, September-October 2020: 42, https://harvardmagazine.com/2020/09/features-a-science-is-born/

19 Lily Kuo, "Hong Kong's Digital Battle: Tech That Helped Protesters Now Used Against Them," *The Guardian*, June 14, 2019, https://www.theguardian.com/world/2019/jun/14/hong-kongs-digital-battle-technology-that-helped-protesters-now-used-against-them.

20 Billy Perrigo, "India's Supreme Court Orders Review of Internet Shutdown in Kashmir. But for Now, It Continues," *Time*, January 10, 2020, https://time.com/5762751/internet-kashmir-supreme-court/.

21 Samuel Woodhams and Simon Migliano, "The Global Cost of Internet Shutdowns in 2019," Top10VPN, January 7, 2020, https://www.top10vpn.com/cost-of-internet-shutdowns/.

22 "Mum-of-Three Uncovered her Cheating Fiance's Double Life After His Wife Came Up as a Friend Suggestion on Facebook," *The Sun*, September 7, 2017, https://www.thesun.co.uk/fabulous/4411305/mum-of-three-uncovered-her-cheating-fiances-double-life-after-his-wife-came-up-as-a-friend-suggestion-on-facebook/.

23 Julia Jones, "Girlfriend Charged in Boston College Student's Death After Telling Him 'Hundreds of Times' to Kill Himself, prosecutors say," CNN, October 29, 2019, https://www.cnn.com/2019/10/28/us/boston-college-student-suicide-charges/index.html.