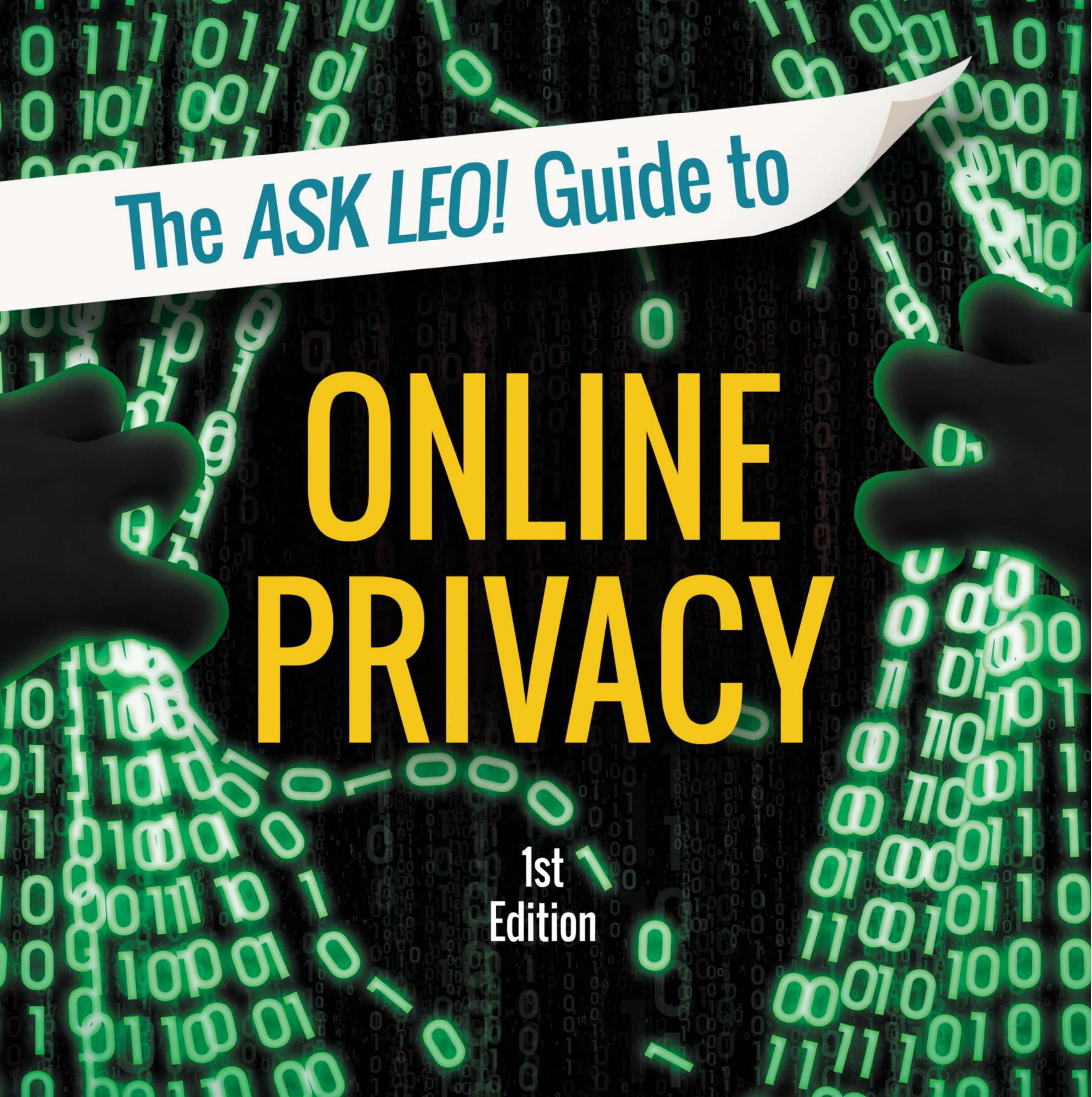


The *ASK LEO!* Guide to

ONLINE PRIVACY

1st
Edition

askleo.com

LEO A. NOTENBOOM

The *Ask Leo!* Guide to Online Privacy

Protecting yourself from an ever-intrusive world

1st Edition

by

Leo A. Notenboom

An *Ask Leo!*® book
https://askleo.com

ISBN: 978-1-937018-43-6 (PDF)
ISBN: 978-1-937018-44-3 (ebook)
ISBN: 978-1-937018-45-0 (paperback)

CONTENTS

The Ask Leo! Manifesto

I believe personal technology is essential to humanity's future.

It has amazing potential to empower individuals,
but it can also frustrate and intimidate.

I want to make technology work for you.

I want to replace that *frustration* and *intimidation*
with the *amazement* and *wonder* that I feel every day.

I want it to be a *resource* rather than a *roadblock*;
a source of *confidence* rather than *fear*;
a *valuable tool,* instead of a source of *irritation*.

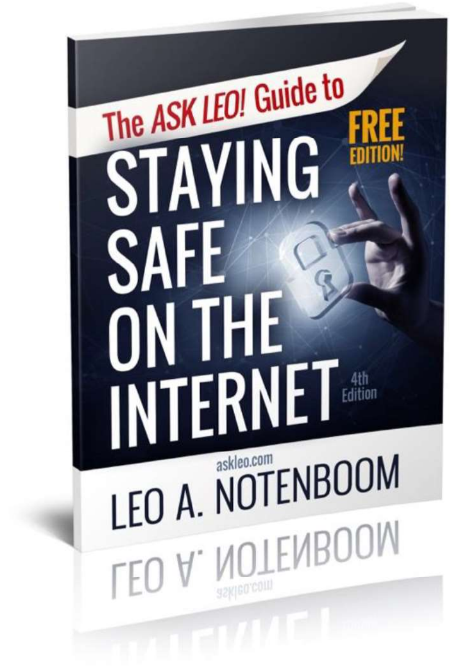
I want personal technology to empower you,
so you can be a part of that amazing future.

That's why *Ask Leo!* exists.

Leo

Leo A. Notenboom
https://askleo.com

First: A Freebie for You



Before we dive in, I have something for you: a copy of ***The Ask Leo! Guide to Staying Safe on the Internet—FREE Edition***. This ebook will help you identify the most important steps you can take to keep your computer, and yourself, safe as you navigate today's digital landscape.

It's yours free when you subscribe to my weekly *Ask Leo!* newsletter.

Each week, you'll find fixes to common problems, tips to keep your computer and online information safe and secure, commentary on technology issues of the day, and even the occasional explanation as to just why things are the way they are. It's educational and fun, and can help you be more effective, more confident, and less frustrated as you use technology.

And it's completely FREE.

Visit https://go.askleo.com/privnews to learn more, browse the archives, and sign up today!

Be Sure to Register Your Book!

Your purchase of this book entitles you to several additional free bonuses.

- All available digital formats of the book as direct downloads. Regardless of which version you purchase, you can enjoy this book on the digital device of your choice.
- Digital updates for life.
- Errata and prioritized Q&A.

You'll find the information you need to register in a chapter near the end of the book. Once you register, you'll be taken to a web page that lists all available bonuses.

INTRODUCTION

Privacy? What Privacy?

Privacy is a *huge* topic. So huge I can't really tell you exactly what steps to take, what settings to change, what apps to avoid, or what services to choose.

Not only are there infinite options, but the options keep changing. In fact, one of the challenges in assembling this book is that I kept coming up with things to ad or update that kept me from pulling the trigger and actually publishing it! (Be sure to subscribe to my newsletter[1] to stay on top of the latest news, updates and information.)

On top of that, there are about as many opinions on the topic as there are internet users. That makes anything I say just one more voice in the crowd …

… not that that's going to stop me. ☺

Two kinds of privacy

"Privacy" is a really big term, and covers many different facets. I want to start by putting a little structure around it. We can lump the various topics two buckets.

Implicit privacy. This is the privacy we assume when we use various online services, modern operating systems, applications, and programs to manage our personal information, data, and activities. Each of them has a set of rules, often codified in some kind of formal privacy policy, that controls exactly what level of access they have to your information, and what they might do with that information as a side effect of your use of their software or service.

Explicit privacy. This is the privacy we control more directly as a result of the choices we make. For example, choosing to share (or not share) a photo on a social media service is one form of explicit privacy, as are the settings we use to control who is allowed to see what we post.

The biggest difference between implicit and explicit privacy, in my mind, is the amount of control we have over it. We implicitly trust that the software and services will do as they say. We explicitly decide what to share based on what we believe may happen.

[1] https://newsletter.askleo.com

Privacy, policies, and Big Brother

The privacy—or lack thereof—assumed when using popular services or software is always a big topic of discussion. For example, Windows 10's activity and tracking generated a great deal of concern as the operating system became more widely used. Whether that concern is warranted is a topic open to debate.

Similarly, using any online service involves some amount of tracking. Visiting a simple web site—even *Ask Leo!*—can result in some amount of what might be considered "tracking", typically in relation to advertising displayed on the site. Some people consider that tracking an invasion of privacy. The most common visible signs are advertisements that appear to follow you from site to site as you navigate the web.

In reality, all the online services and websites you visit have the ability to collect vast amounts of data derived from internet users. Similarly, any and all software you install has the ability to collect usage information.

Whether or not you believe Big Brother is watching, the bottom line is that the technology is there should he want to.

The (poor) choices we make

At the other end of the privacy spectrum are the often poor choices we make about what information we share and with whom.

I regularly hear from individuals who share a password with a trusted friend or significant other, only to be surprised when their privacy is violated in some way because that trust was unwarranted.

We've all heard stories of individuals losing jobs or job opportunities for statements made, or photos or videos posted on social media. Call your boss names on Twitter, for example, and you have no one to blame but yourself when you're shown the door the next morning. Have you posted "funny" pictures of yourself after imbibing a tad too much alcohol? That could easily be the reason you're not hired for the next job you apply for, or don't get the loan you applied for.

It's sadly common that when it comes to privacy, we're often our own worst enemy.

You're just not that interesting

I've said it over and over: you and I just aren't that interesting as individuals. That your operating system might track what you do is pretty meaningless in terms of personal privacy. That advertisers might use your browser history and things you click on to tailor what you see is similarly pretty benign.

The companies that collect this data aren't looking at you as an individual. They're looking for trends, accumulated data on thousands (if not millions) of users to determine what's being acted on, what's influencing people, and what they might do better.

Even I do it. For example, do I care that you, specifically, looked at my newsletter? At some personal level I do, but I'm not going to sift through information on nearly 60,000 subscribers to see who did and who didn't. On the other hand, if the aggregate number of people who open my newsletter changes in some dramatic way, that's a sign I want to see; that's information I want to act on. I can only do that by tracking the behavior of 60,000 individuals.

The same is true for most any company. Your privacy isn't being violated, because nobody is looking at you, specifically. You're just not that interesting.

But you might be interesting to someone, someday

There are two cases in which you might become "interesting".

If you run afoul of the law. This is a non-issue for most people. But what if you live in an oppressive regime, or are subject to investigation for your activities by whatever law enforcement agencies apply to your situation? Even this falls into two sub-categories: the unduly paranoid (sadly, a larger number than one might hope), and the legitimately concerned, for both legal and illegal reasons.

It is important to realize that if you fall into this category (again, depending on where you live), law enforcement may have the right to collect information about you. This can include information we normally brush off as irrelevant, like ad or service usage information collected by your ISP, or the services and software you use. I have to say law enforcement *may* have the right, because laws differ dramatically depending on where you live. Of more practical import, perhaps, law enforcement capabilities also often vary dramatically based on everything from expertise to budget to prioritization of where they choose to expend their limited resources.

Future opportunities. The other case is the one I alluded to earlier: some years from now, perhaps someone will research your history as part of a job application, or something else where your record and your reputation are important. What you post