Privacy Matters !

PRIVACY IN DIGITAL ERA

Everything you do leaves a footprint somewhere.

RICHARD WHITE

Privacy in Digital Era

Everything you do leaves a footprint somewhere.

Richard White

This book is for sale at http://leanpub.com/Privacy_in_Digital-Era

This version was published on 2014-06-11

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Tweet This Book!

Please help Richard White by spreading the word about this book on Twitter!

The suggested hashtag for this book is #Privacy in Digital Era.

Find out what other people are saying about the book by clicking on this link to search for this hashtag on Twitter:

https://twitter.com/search?q=#Privacy in Digital Era

Also By Richard White

Anonymity in Digital Era

Contents

Introduction

Today significant part of our communication takes place over the Internet, mainly through the services of different corporations.

Our digital lives are being recorded, it's the reality of the world we live in.

Every day, corporations & agencies around the world are recording lives of millions, they collect massive amounts of information about who we know, where we've been, and what we've done.

This surveillance apparatus can track the location of hundreds of millions of people, collect the phone records of the entire nation, and tap into the very backbone of the internet Is collecting millions of electronic records belonging to people who are not suspected of any wrongdoing.

The manner in which we use the internet influences our lives, data once written on the web stays on the web.

As a user, you need to be aware of risk, and the specific threats that are related to your methods of communication via Internet. Some of these risks are different, but as long as you're aware of them, you can manage them. And manging that risk is a very important part of privacy.

What is privacy

Privacy is not only the right but also the natural need of every human being. Every person has the inalienable right to anonymity and privacy of communication.

Definition of privacy by Oxford dictionary:

A state in which one is not observed or disturbed by other people:

The state of being free from public attention:

Everyone has the right to free activities on the Internet without anyone's control over it. Regardless of whether or not you have something to hide, protecting your privacy is a matter of principle, it's about accessing data without your knowledge and consent for reasons unknown.

About the book

Privacy in Digital Era is a practical, pragmatic guide with one intent, to show you methods you can use to protect your privacy.

Hopefully, you'll go places you've never been and see things you've never seen, the content of this book is meant to be experienced. To be used.

You'll learn how to:

- Harden your system security.
- Monitor malicious activities.
- Properly handle data erasure.
- Encrypt your storage to prevent someone from accessing the sensitive data on your hard drive and cloud services.
- Prevent others from viewing your private browsing and conversations.
- Encrypt your internet traffic.

Book formats & versions available

The book is currently available in pdf, epub and mobi format, all included in the same price! The epub and mobi formats are best for reading on dedicated e-readers. Even if you are reading it on an e-reader, you may wish to download the PDF version as well for use on your computer.

Being published on leanpub.com[1], this book can easily be revised and updated. You will automatically be notified about any updates in the future.

Whichever versions you use, you will always get free access to all future updates to the e-book.

Author's website[2]

[1] https://leanpub.com/u/jdoe

[2] http://digital-era.net

An important note for Windows and Mac users

Software solutions discussed run on Windows, Mac OS X, and Linux operating systems.

For encryption that means files encrypted on one of operating systems are completely compatible with other and can be decrypted on it.

There is something else I want to bring your attention to!

To effectively use information provided in this book you should consider giving Linux a go. You need a reasonably secure system from which you can use Tor and reduce your risk of being tracked or compromised.

If for some reason you are unable to set up Linux, use Tails or Whonix (we covered Whonix in chapter titled "Encrypting your Internet traffic") instead, where most of this work is done for you. It's absolutely critical that outgoing access be firewalled so that third party applications cannot accidentally leak data about your location.

> **Few thoughts from Richard Stallman[3]**
>
> > Without Richard Matthew Stallman, who founded the Free Software Movement[4], there would be no GNU, and without GNU there would be no Linux distributions as we know them today.
>
> People who use proprietary software [programs whose source code is hidden, and which are licensed under exclusive legal right of the copyright holder] are almost certainly using malware. The most widely used non-free programmes have malicious features – and I'm talking about specific, known malicious features.
>
> There are three kinds: those that spy on the user, those that restrict the user, and back doors. Windows has all three. Microsoft can install software changes without asking permission.
>
> When people don't know about this issue they choose based on immediate convenience and nothing else. And therefore they can be herded into giving up their freedom by a combination of convenient features, pressure from institutions and the network effect.
>
> A proprietary programme gives you zero security from the owner of the programme. The users are totally defenceless and the owners often wipe the floor with the users because every non-free program gives the owner unjust powers.
>
> People are aware that Windows has bad security but they are underestimating the problem because they are thinking about third parties. What about security against Microsoft? Every non-free program is a 'just trust me program'. 'Trust me, we're a big corporation. Big corporations would never mistreat anybody, would we?' Of course

[3] http://en.wikipedia.org/wiki/Richard_Stallman

[4] http://www.fsf.org/about/

they would! They do all the time, that’s what they are known for. So basically you mustn’t trust a non free programme.

Conventions used in this Book

There's several conventions used through this book.

This is a Warning

You should really pay attention here, otherwise be prepared to deal with the consequences.

This is a Tip

Usually a piece or two of useful information.

This is an Information box

Special information here.

Terminology

I'll use some acronyms in this book. The first time I use an acronym, I'll write its expanded form in parenthesis, like this: AAG (Acronyms Are Great).

For your convenience, here's a short list of acronyms, abbreviations, and potentially confusing terms that I use in this book:

CLI Command-line interface. A textual interface to a tool that is meant to run on the command-line.

GUI A graphical user interface.

OS Operating System.

Current situation

We live in a time when a significant part of communication takes place over the Internet, to be more precise a substantial part of Communication takes place through services of different corporations. Facebook, Google, YouTube, Twitter, Skype are some of the services which we now use to interact with millions. Bear in mind that most of them are products of multinational corporations, and only the naive could believe that the government is not deeply involved in monitoring and capturing data.

Companies cooperate with intelligence agencies, they are collecting data on the activities on the Internet and over mobile networks thus contributing to a system of mass surveillance. Various corporations and other institutions mainly do it with intention to make money, either by using them to optimize their marketing and sales strategies, or by selling them to other entities who want to use them for the similar purpose.

Imagine for a moment that every conversation and every form of communication in the world is accessible to them. These companies collect information about your searches over the internet, who contact´s who, manner in which you communicate as well as content of communication, they know who your friends are, what you like, dislike, what are your political views, religious views, etc.

Even by monitoring via cell phone through the base stations (or over GPS) over a couple of months can determine in detail your lifestyle, the area in which you move, where you were and will be during the day. Lots of other data is collected and all this can be very easily abused.

Lets not forget the interconnectedness of various online services that we use, someone malicious could with relatively little effort create huge mess in our virtual world.

Why would someone in this “social” age want to be anonymous? Simple - the more information you share about yourself without thinking, you run the greater risk: financial, reputational and various others.

The situation is not particularly reassuring, however with a little caution, discipline, use of common sense and some corrective action it is possible to keep things under control.

We are being watched

Intelligence services are more or less in control of the Internet and general communication. Many people have suspected for years that the intelligence services of the most powerful states implement global control, as recently confirmed by now former NSA employee Edward Snowden.

Mr. Snowden decided to go public with information about the NSA global system for monitoring the Internet and other communication systems through Prism, XKeyscore and Tempora. Edward Joseph Snowden, submitted sensational documents to British newspaper The Guardian[5] and the U.S. The

[5] https://duckduckgo.com/?q=site%3Atheguardian.com%20snowden

Washington Post[6] concerning loss of privacy and degree of control over information.

Thanks to Snowden, numerous “conspiracy theories” now become irrefutable facts.

A worrying phenomena is the attitude of a growing number of people who simply do not care that they were tapped and that their activities and communications are being monitored and reviewed. More and more people have the attitude of “let them listen, i have nothing to hide.”

How might our online habits be used against us?

This is where things get interesting…

[6] https://duckduckgo.com/?q=site%3Awashingtonpost.com+snowden