Solve your problem with a wink

My Address Is Traveling the Internet Without a Suitcase

How to Find Where Your Personal Data Appears and Reduce Its Public Visibility



Max Paradox

My Address Is Traveling the Internet Without a Suitcase

How to Find Where Your Personal Data Appears and Reduce Its Public Visibility

Max Paradox

PROBLEM? RELAX. YOU'VE GOT THIS!

ISBN: 9788384905203

ALL-IN Rafał Płonkowski



CONTENTS

INTRO 5

Chapter 1 - Your Personal Data Has a Busier Social Life Than You Do 11

Chapter 2 - Who Handed Out My Personal Data, and Why Did Nobody Ask? 19

Chapter 3 - The Biggest Privacy Mistakes, or How to Become Your Own Informant 28

Chapter 4 - Magic Buttons Don't Exist, and the Internet Doesn't Have an Eraser 37

Chapter 5 - Digital Clutter, or How to Find a Needle in a Haystack of Your Own Data 46

Chapter 6 - Dead Accounts Live On, or Digital Ghosts from Years Gone By 55

Chapter 7 - Family, Friends, and Other Unofficial Spokespeople for Your Life 65

Chapter 8 - Default Settings, or Privacy Hidden Behind Three Menus 74

Chapter 9 - Operation: Find Me Before Someone Else Does 83

Chapter 10 - Would You Kindly Disappear? How to Write an Effective Data Removal Request 92

Chapter 11 - The Search Engine Doesn't Own Your Address, but It Can Stop Advertising It 102

Chapter 12 - Registers, Directories, and Official Documents: When Privacy Meets the Rubber Stamp 110

Chapter 13 - Digital Business Card Factories, or How to Unsubscribe from a Directory You Never Joined 121

Chapter 14 - New Address, New Rules: How to Avoid Scattering Your Data Again After the Big Cleanup 130

Chapter 15 - The Administrator Has Disappeared, the Server Is Silent, and Your Address Is Still Online 139

Chapter 16 - When Your Address Becomes a Weapon and Privacy Stops Being Just Another Setting 148

Chapter 17 - Not Everything Can Be Deleted, or the Art of Winning Without Erasing the Entire Internet.....158

Chapter 18 - Privacy After the Big Cleanup, or How to Avoid Returning to Square One 168

Chapter 19 - An Alarm Without a Siren, or How to Recognize When Your Data Is Traveling Again 178

Chapter 20 - Your Address Doesn't Need a Full-Time Babysitter.....188

INTRO

Imagine that one quiet evening, you type your full name into a search engine. You do it out of curiosity, perhaps out of boredom, or maybe because someone told you it was worth checking what the internet knows about you. You expect to find a professional profile, a few comments, and an old photograph in which you look as though your hairdresser had a personal grudge against you. Instead, among the search results, you spot your address. The whole thing. Street name, house number, and postal code. The only detail missing is what time you usually go out to buy bread rolls.

You stare at the screen, wondering who exactly gave your address permission to launch an international career. After all, you never sent it anywhere. At least, not knowingly. You didn't create a social media account for it, buy it a ticket, or give it permission to make public appearances without supervision. Yet there it is, available to people you don't know, haven't invited over, and wouldn't normally trust with so much as your intercom number.

The first reaction is often anger. The second is panic. The third is the sudden urge to erase yourself from the entire internet, throw away your phone, and begin a new life under an assumed name in a town that doesn't appear on any map. Unfortunately, even if you moved into the middle of a forest, someone would probably publish your details in an online directory of landowners. So rather than planning a dramatic relocation, it makes more sense to understand where this information comes from and what you can actually do about it.

Because the internet isn't one enormous filing cabinet from which you can simply remove the sheet bearing your name. It's more like a vast residential neighborhood where every building has its own administrator, some residents keep copies of documents, and others pin people's personal information to public noticeboards because, at some point, they decided they were entitled to. Even when one noticeboard is cleared, the same information may still be hanging three streets away.

Your address might have appeared in an old sales advertisement, a business profile, a public register, a document archive, or a website you'd forgotten existed. Your phone number might have found its way into a contact directory. Your email address might have been published alongside an event, a comment, or your professional activities. Sometimes the information comes from lawful, publicly accessible sources. At other times, its publication results from a mistake, outdated privacy settings, or the actions of an organization that shouldn't have made it available in that way.

The most irritating part is that an individual piece of information doesn't always look dangerous. Your first name? Hardly a disaster. The name of your town? Plenty of people live there. A photograph of your building? Lovely facade, congratulations. It's only when these little details are combined that they begin to form a remarkably accurate picture of a person. The internet can assemble such puzzles with the patience of a retiree working on a five-thousand-piece jigsaw depicting nothing but blue sky.

That doesn't mean, however, that every public mention of you represents a threat. This is an important distinction because, without it, sensible privacy protection can very

easily turn into an endless hunt for your own name. The fact that someone can find a piece of information doesn't automatically mean anyone intends to use it against you. There is, nevertheless, a fundamental difference between consciously sharing your details and having absolutely no idea who published them, why they did so, or how long they intend to keep them.

Regaining that understanding is precisely what this book is about.

We're not going to pretend that there's a magical "Delete Me from the Internet" button that makes every server in the world politely forget your name. If such a button actually worked, its inventor would have a queue of customers stretching all the way to the Moon. Instead, we'll examine practical ways to search for your personal information, identify where it's been published, assess the risks, and take steps that may reduce its visibility.

You'll learn to distinguish between a website that stores information and a search engine that merely points people toward it. That distinction matters enormously. Removing a search result doesn't necessarily mean the information has disappeared from the original website. Equally, deleting information at its source doesn't guarantee that every link, copy, and earlier trace will vanish immediately. In practice, you may sometimes need to contact a website administrator, sometimes use a search engine's removal form, and sometimes establish whether there are legal grounds for requesting that the processing of your personal data be restricted or that the data be erased.

Sounds terribly bureaucratic? Relax. I have no intention of turning this book into an instruction manual for a filing cabinet labeled "Procedures, Attachments, and Other

Reasons to Lose the Will to Live." The point is to help you understand whom to contact, how to phrase a reasonable request, and what to do if the first response amounts to: "Thank you for your message, but no."

Another important part of our work will be setting priorities. Not every piece of information requires an equally urgent response. A publicly listed phone number used for professional purposes is a different matter from a private residential address connected to details about family members. An outdated entry on an obscure website may carry different implications from a result that appears on the first page of a search engine when someone enters your surname. We'll consider not only what is visible, but also who can access it, the context in which it was published, and the real-world consequences that might follow.

Not everything can be removed. Some information remains public because of legal requirements, obligations relating to official registers, or the legitimate interests of other parties. Sometimes a request will be refused because there are no grounds for granting it. At other times, information may disappear from one website while remaining accessible elsewhere. None of this is a reason to give up. Making private information harder to find can still be valuable, even when it doesn't result in the complete disappearance of your digital footprints.

We'll also examine habits that unintentionally increase our visibility. Sometimes a person spends three hours trying to remove their address from an online directory, then posts a photograph of a parcel with the shipping label clearly visible. Or carefully hides their phone number while leaving it in a public advertisement from six years ago. The aim isn't to point fingers at these mistakes. It's to understand that

privacy is the result of many small decisions, not a single act of digital heroism.

Naturally, we'll stick to legal and safe methods. There's no need to hack into databases, purchase suspicious reports, or hand over your identity document to the first website promising to delete everything in five minutes. Paradoxically, a careless attempt to protect your privacy can result in even more information being exposed. That's why checking the credibility of the organization receiving your removal request will be just as important as locating the information itself.

This book is not a substitute for personalized legal advice or professional security assistance. If the exposure of your personal information is accompanied by threats, harassment, identity impersonation, or immediate danger, the situation may require urgent action beyond simply cleaning up search results. In other circumstances, a methodical approach is usually more sensible than sending thirty identical messages WRITTEN ENTIRELY IN CAPITAL LETTERS.

For now, all you need is a change of perspective. Instead of asking, "How can I disappear from the internet?" ask, "Which pieces of my personal information are publicly accessible, where did they come from, and what can I realistically control?" The first question usually leads to frustration. The second allows you to take concrete action, evaluate the results, and make informed decisions about what deserves your attention first.

Your address doesn't need a passport, its own website, or another season of a travel documentary series. You may not regain control over every place it appears, but you have a

real opportunity to understand its digital itinerary far better and eliminate some of its unnecessary stops.

And that's already a pretty good beginning. Especially because, this time, you're the one organizing the trip.

Chapter 1 - Your Personal Data Has a Busier Social Life Than You Do

If your personal data had its own calendar, there probably wouldn't be a single free appointment in it. On Monday, it makes an appearance in a business directory. On Tuesday, it visits an archived advertisement. On Wednesday, it turns up in a search engine, and by Thursday, someone has discovered it on a website whose name you can't even pronounce. Meanwhile, you're sitting peacefully at home, convinced that because you haven't updated any public profiles in three years, the internet has probably forgotten all about you. Unfortunately, the internet isn't an acquaintance who stops calling after a few unanswered attempts. It's more like an archivist with an obsessive compulsion to preserve absolutely everything that has ever crossed their desk.

Let's begin, however, with an important distinction. The fact that your data exists somewhere doesn't automatically mean it's public. An online store may keep your delivery address in its order management system, a bank may hold your identification details, and a medical clinic may possess information about your health. Simply storing that information, provided it is appropriately protected and handled in accordance with the law, is not the same as making it available to everyone who visits a website. The problem begins when information travels beyond its expected audience or appears somewhere much easier to access than you had anticipated.

Imagine Anna, who ran a small business several years ago. When registering the company, she provided an

address associated with her business activities, which also happened to be her home address. Eventually, she closed the business, changed jobs, and stopped paying attention to the old listings. One day, a friend tells her that searching for her surname reveals her street and building number. Anna is surprised because she considers that information private. The internet, however, has its own definition of the word "long ago." As far as it's concerned, five years is barely enough time to redesign a homepage.

In situations like this, it's easy to confuse three separate things: the existence of information in a particular source, its accessibility to outsiders, and its visibility in search results. Information may be publicly available but difficult to find. Alternatively, a search engine may display it almost instantly, even though it comes from a document published many years earlier. Each situation requires a different way of thinking. Unless you establish which one you're dealing with, you could spend an entire evening fighting the wrong opponent.

What exactly makes up your digital footprint?

When most people hear the term "personal data," they imagine a first name, surname, address, and telephone number. That's a sensible starting point, but the list is considerably longer. Personal data means information relating to an identified natural person or someone who can be identified, including indirectly. Under certain circumstances, it can include online identifiers, location information, or a combination of details that only reveal someone's identity when brought together.

In practice, this means your online presence consists of information with varying degrees of identifiability. An email address containing your surname may identify its owner

directly. A nickname used exclusively in one computer game might not reveal your identity until someone connects it to other profiles. A photograph of a house may mean very little on its own, but place it beside a full name and building number, and the situation changes. The internet is exceptionally good at connecting fragments that the people who originally published them never intended to combine.

It's also worth remembering that your digital footprint doesn't emerge exclusively from things you publish yourself. Information can come from other individuals, organizations, or institutions. Someone tags you in a photograph, posts a list of event participants, publishes a document containing your name, or leaves an entry in a directory. Some of these publications are justified and lawful, while others may be unnecessary or problematic. The fact that you weren't sitting at your computer when they appeared doesn't stop the process. Unfortunately, personal data doesn't need written authorization to become the subject of somebody else's website.

Nor does everyone have the same kind of digital footprint. Someone running a business may appear in official registers and industry directories. A person involved in local organizations may be mentioned in announcements and reports. Someone else may have left more information through publicly accessible social media profiles. Every case has its own history, which is why a universal list of websites you should remove yourself from quickly proves less useful than knowing how to recognize the sources of your information.

There's also a difference between current and historical information. An old telephone number may no longer belong to you but still appear beside your name. A previous address

may lead to an apartment occupied by someone else for years. Such information can cause problems not because it accurately describes your present circumstances, but because it may mislead other people. The internet doesn't always understand that human lives change faster than a directory last updated around the launch of a long-forgotten mobile phone.

Your first encounter with your own name

Start your simplest privacy audit with an ordinary search engine, without creating accounts with random services promising comprehensive reports about your entire existence. Enter your first name and surname inside quotation marks, then examine the results. Quotation marks may help locate an exact phrase, although the behavior of search operators varies between search engines. If your surname is common, add your town, the name of a former business, or another detail you already know. Don't attempt to search the entire internet immediately. Your first objective is to establish what information can be found through simple, natural searches.

Why does this matter? Because that's exactly how someone who knows your name might look for information about you. They don't need specialist software or skills borrowed from a spy film. A few words and a little patience are enough. However, if a result concerns someone who happens to share your name, don't automatically assume it's about you. Poland has enough Kowalskis, Nowaks, and Wiśniewskis for mistaken identities to qualify as a separate national sport.

As you examine the results, look for details that can confirm the person's identity. These might include a former workplace, a town, an association with an organization, or an

address you recognize. If those elements are missing, leave the result marked as unverified. It's better to have one entry on your list with a question mark beside it than to start corresponding with a website administrator, demanding the deletion of information belonging to a person whose only offense is having the same surname as you.

Pay attention to the snippets of text displayed beneath search results as well. Sometimes a search engine shows an address or telephone number in these snippets even though the information is difficult to locate after opening the page. The snippet may come from an earlier indexing of the website or from a section that isn't immediately visible. Nevertheless, don't treat a short search description as sufficient proof of the website's current contents. Open the result, examine the page, and make a note of what is actually visible.

Keeping a simple record of your discoveries is a good idea. A document or spreadsheet containing the page address, the type of information found, the date you checked it, and a brief description of the publication's context is enough. Also record whether the information appears directly on the website or only in the search engine's description. This record doesn't need to resemble the evidence files of an international investigative agency. Its main purpose is to prevent you from searching for the same page again next week because you vaguely remember finding it "somewhere between a business directory and that weird website with the green logo."

If you take screenshots, store them sensibly. After all, they contain precisely the information whose visibility you're trying to reduce. Don't place them unnecessarily in public folders or send them to random people. A protected local

folder or another trusted storage location will often be sufficient. It would be rather amusing if documenting the exposure of your personal data resulted in publishing yet another copy of it, but only from the perspective of someone writing a comedy.

Visibility doesn't always mean danger

After your first review, you may discover a dozen or more results that concern you in some way. The natural reaction is: "Delete everything!" Before launching a full-scale digital cleanup operation, however, consider which pieces of information actually matter. A public article mentioning your name as a participant in an event is different from a page containing your current private residential address and telephone number. Both publications may be easy to access, but their consequences are not necessarily comparable.

A practical assessment begins with three questions. How precise is the information? How easily can it be connected to you? And what could someone who discovers it potentially do with it? A full residential address identifies a specific location. The name of your town is considerably less precise. A telephone number may make unwanted contact easier. An old nickname that nobody associates with your real identity may matter very little, unless it provides a route to other personal details.

You don't need to assign every discovery a mathematical risk score. It's enough to divide your findings into those requiring urgent attention, those worth checking later, and those that don't currently justify action. If you discover your current home address combined with information that could facilitate harassment or impersonation, the situation may require a swift response. If you find a caption beneath a

photograph from an old conference, you can probably finish your cup of tea first.

It's also worth distinguishing discomfort from a specific threat. You have every right to dislike excessive visibility of your personal information, even when no misuse has occurred. At the same time, not every unwanted publication is illegal, and not every piece of information can be removed on request. Whether such a request is justified depends, among other things, on the source of the information, the purpose of its processing, and the applicable regulations. In more complicated situations, consulting a data protection specialist may be helpful.

Your first audit should end with organized knowledge rather than a feeling of defeat. Even if you uncover more information than you expected, finding it gives you the opportunity to act consciously. Until now, those details may have existed completely outside your awareness. You now know at least some of the places where they appear and can assess their significance.

Don't turn a single evening into an endless investigation, though. Set a reasonable amount of time for searching, record the results, and finish the task. A search engine will always have another page of results, another variation of your query, and one more link suggesting that perhaps something important is hiding just beyond it. If you allow the search engine to decide when the job is finished, you'll probably replace your computer before you manage to close all the browser tabs.

The most important outcome of this initial investigation is simple: you stop treating your online presence as one enormous, mysterious whole. Instead, you begin to see specific pieces of information, identifiable sources, and

different levels of accessibility. This allows you to distinguish a genuine problem from the mere fact that the internet remembers your name.

Your personal data may still have an extraordinarily busy social life. At least you now know which parties it has been attending without your knowledge.

Chapter 2 - Who Handed Out My Personal Data, and Why Did Nobody Ask?

At some point, almost everyone trying to sort out their online privacy reaches the same conclusion: "But I never published this information!" That statement may be perfectly true, yet it doesn't solve the mystery. Personal data can travel to new places without you publishing it again, and its presence isn't always the result of one easily identifiable event. Sometimes the process resembles the history of a family recipe passed on to five people, each of whom changes the ingredients, until several years later nobody remembers where the dish originally came from. The difference is that a cheesecake recipe rarely includes someone's residential address.

Imagine Marek, who put his car up for sale a few years earlier. In the advertisement, he included his telephone number, town, and first name. He sold the vehicle, the advertisement expired, and Marek considered the matter closed. Some time later, however, he discovers a website displaying archived listings. There are photographs of his car and his former contact number. At this stage, nobody knows whether the information was copied in accordance with the original website's terms or republished in violation of particular rules. What is clear is that the expiration of the advertisement did not automatically make every copy disappear.

Situations like this reveal an important characteristic of how information circulates online: the original source and its

current place of publication don't have to be the same. Data provided to one organization may subsequently be shared, indexed, archived, or copied by another. Each of these processes has its own causes and legal limitations. That's why it's useful to break the question "Who published my personal data?" into two more precise questions: where did it first appear, and who is currently responsible for making it available?

From an online form to a public directory

Think back to the last online form you completed. You probably wanted to order something, book a service, or create an account. You provided information because it was necessary for a particular purpose. At some point, you may have encountered a privacy notice, terms and conditions, or a collection of consent options. If the form was particularly ambitious, the accompanying documentation was long enough to serve as a wedge beneath a wobbly table.

Not every type of personal data processing requires consent. Data protection legislation provides several possible legal grounds, including the performance of a contract, compliance with a legal obligation, and, under certain conditions, legitimate interests. However, providing an address for delivery doesn't automatically amount to permission to publish it in a public directory. The purpose of processing matters, as do the scope of the information and the people or organizations to whom it is disclosed.

In practice, many misunderstandings arise precisely because different purposes become confused. A business owner may have provided an address in connection with their commercial activities, only to discover it later on a website aggregating publicly available company information. Someone registering for an event may subsequently find