“We all need to protect our digital privacy. This book provides real-world examples and the guidance we need to protect ourselves and our loved ones.”

JOHN LEE DUMAS

PRIVACY CRISIS

WORKBOOK

CHRIS PARKER

INTRODUCTION

Privacy isn't just a concern anymore—it's a full-blown crisis. Your data is constantly being tracked, collected, and exploited. But locking down your privacy doesn't mean going off the grid or making your life miserable. You don't have to delete every account, abandon your smartphone, and move to a cabin in the woods.

What do you need? A plan.

That's where this workbook comes in. It is intended to be a companion for readers of Privacy Crisis by Chris Parker. Privacy Crisis is filled with actionable strategies to avoid scams, secure your devices, accounts, and identity, and stop data brokers, hackers, and corporations from exploiting your information.

This workbook is your personal privacy playbook, designed to help you go from "I should really do something about this" to actually securing your digital life.

No fluff, no fearmongering—just practical steps to take back control.

Inside, you'll find exercises to help you spot vulnerabilities, rethink your digital habits, and put real privacy protections in place—without turning your daily routine upside down. Some will take minutes, others a little longer, but each one is designed to move you closer to a safer, more private online presence.

The goal isn't to disappear.
It's to stay visible on your terms.

Let's get started.

—Chris Parker

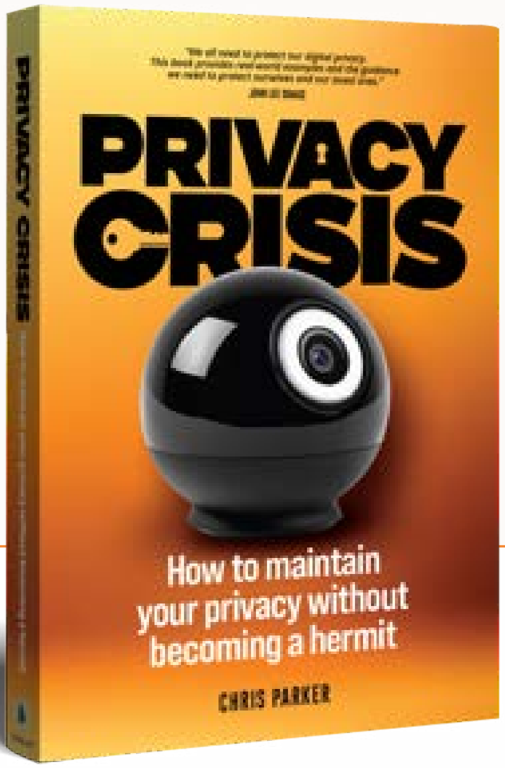
CHAPTER 1

IMMEDIATE ACTIONS TO INCREASE SECURITY

It’s time to protect your privacy and increase your security online. Ready to get started?

In this workbook chapter, you will:

- ✓ Review key concepts from Chapter 1 of Privacy Crisis
- ✓ Identify your own personal motivations for improving your privacy and security
- ✓ Consider which action steps may be the most challenging for you
- ✓ Complete the 8 essential actions described in Chapter 1



ACTIVITY 1

Let’s start with a quick brainstorm.

Take a moment to jot down your thoughts - don’t worry, we’ll guide you through the details later in this workbook. For now, just get your ideas down on paper.

Why do you want to improve your privacy and security online?

In Privacy Crisis, we learned that privacy and security are closely related concepts, but there are differences between them.

- Privacy keeps your information hidden.
- Security keeps your information safe.

If you improve one of these areas, the other area benefits, too. Here are some of the reasons why people choose to improve their privacy.

Check off the ones that are important to you.

- □ Being at risk of identity theft and fraud
- □ Being targeted for financial theft or scams
- □ Being the subject of stalking and harassment
- □ Having personal information exposed in data breaches
- □ Becoming a target for swatting or doxxing
- □ Being manipulated into overspending through targeted advertising
- □ Having your behavior and choices influenced by personalized content algorithms
- □ Being targeted with disinformation or propaganda based on your data profile
- □ Developing addictive behaviors encouraged by engagement algorithms
- □ Losing job opportunities due to exposed personal information
- □ Having private information used against you in legal situations
- □ Being harassed or targeted at work based on leaked data
- □ Having medical or health information exposed
- □ Having relationships damaged by exposed private details
- □ Having your information remain accessible even after you try to delete it
- □ Being unable to control how companies buy, sell, and share your data
- □ Facing unknown risks as technology and data collection methods advance

Did you find yourself checking most or even all of the boxes? You might have even found yourself checking off items that you didn't even realize were a problem!

ACTIVITY 2

Let’s start with a quick brainstorm.

Take a moment to jot down your thoughts - don’t worry, we’ll guide you through the details later in this workbook. For now, just get your ideas down on paper.

What changes will be difficult for you to make?

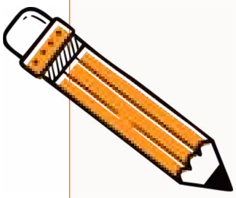
You can do these in whichever order you want! If you want to start with the easiest ones, that’s a great plan! If you want to start with

Chapter one asks you to complete several steps you can do *right now* to increase your privacy and security online. Some of these tasks may seem super easy to you, but people often struggle with at least a few. Maybe these tasks feel inconvenient or unnecessary. It could be that you are not sure that you have the technology skills to make each one happen.

Regardless of why some of these might be difficult for you, facts are facts: These are the action steps you can take to be safer *right now.*

Checklist

RANK THESE 8 ACTIONS IN ORDER OF EASIEST TO MOST CHALLENGING FOR YOU.



□ Completely shut down/power off your smartphone for at least five minutes.

□ Lock your mobile phone SIM through your wireless service provider.

□ Encrypt all of your computers and mobile devices.

□ Get a zero-knowledge password manager and migrate all of your account credentials and other secret information to it.

□ Freeze your credit files with Experian, Equifax, and Transunion.

□ Enable one or more methods of strong two-factor authentication for your primary single sign-on account.

□ From now on, distrust by default any request for payment or to change the method of payment, no matter who it seems to be from.

□ Don’t unlock or use your phone in a crowded place, and never let anyone borrow it.

ACTIVITY 3

Let's start with a quick brainstorm.

Take a moment to jot down your thoughts - don't worry, we'll guide you through the details later in this workbook. For now, just get your ideas down on paper.

Accomplish all 8 immediate actions to safeguard your data online

You can do these in whichever order you want! If you want to start with the easiest ones, that’s a great plan! If you want to start with the harder ones and reward yourself with easy steps at the end, you can totally do that, too!

However, if you want to be safer online and avoid those pitfalls from Activity #1, it’s time to get started on these 8 steps.

Use these checklists to make changes to your privacy habits and security standards.

Power Off Your Smartphone

WHY: Shutting down your smartphone for 5 minutes clears potentially harmful malware from your phone's temporary memory that could be recording your activity.

- □ **Save any open work**
- □ **Close all apps**
- □ **Hold the power button until shutdown options appear**
- □ **Select "Power Off" or "Shut Down" (not Restart)**
- □ **Wait 5 full minutes**
- □ **Power the phone back on**

Lock Your Mobile SIM

WHY: Locking your phone's SIM prevents thieves from transferring your phone number to their device and intercepting your calls, texts, and 2FA codes.

- □ **Locate your carrier's website or app**
- □ **Log into your account**
- □ **Navigate to security settings**
- □ **Find SIM card or device security section**
- □ **Enable SIM lock/PIN**
- □ **Store SIM PIN securely**
- □ **Test to see that it works**

Encrypt Your Devices

WHY: Strong encryption makes your data unreadable to thieves—even if they physically steal your device.

If you're not sure where to get started, check out the instructions in Privacy Crisis under the "Encrypt Your Devices" heading.

Check the current encryption status on each device and enable encryption:

- □ **smartphones**
- □ **tablets**
- □ **laptops**
- □ **desktop computers**

- □ **Verify encryption is active**

Create a secure backup of recovery keys (stored in a password manager, locked in a fireproof safe)

An important reminder: Never store your recovery keys in a digital photo, in the cloud, in an email, in a notetaking app, or in non-encrypted computer files.

Set Up Your Password Manager

WHY: A password manager securely stores all your passwords and sensitive information, making them inaccessible to thieves.

- □ Research recommended password managers, such as Bitwarden, Proton Pass and 1Password
- □ Choose a zero-knowledge service
- □ Create master password
- □ Install desktop application
- □ Install mobile app
- □ Enable sync between devices
- □ Begin importing existing passwords
- □ Set up emergency access if needed

Freeze Credit Files

WHY: Freezing your credit prevents criminals from opening new accounts or taking loans in your name.

- □ Visit Experian's website and follow the site's instructions to complete an Experian freeze
- □ Visit Equifax's website and follow the site's instructions to complete an Equifax freeze
- □ Visit TransUnion's website and follow the site's instructions to complete a TransUnion freeze
- □ Save the confirmation details of each freeze
- □ Take note of the procedures to unlock each credit file later, when you need to

Enable Strong 2FA

WHY: 2-factor Authentication adds an essential second layer of security, even if someone gets your password.

- □ Identify your main account (Google, Apple, etc.)
- □ Review available 2FA options
- □ Choose the strongest available method
- □ Enable your primary 2FA method
- □ Set up a backup 2FA method
- □ Safely save/store backup codes
- □ Test both 2FA methods
- □ Document recovery process

Create Payment Verification Process

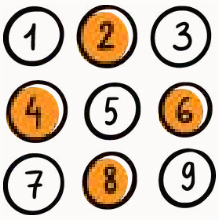
WHY: Protects you from scammers trying to steal money through fake payment requests.

- □ List all your legitimate payment methods
- □ Document normal payment processes
- □ Create a verification checklist
- □ Save official contact numbers

Adjust Your Phone Security Habits

WHY: Good phone security habits prevent unauthorized access to your unlocked device.

- □ Set your auto-lock to shortest practical time
- □ Use a strong unlock method
- □ Commit to always being aware of the surroundings
- □ Keep your screen hidden when possible
- □ Never leave your phone unattended
- □ Decline requests to borrow your phone
- □ Log out of sensitive apps when done
- □ Conduct regular security audits



CHAPTER 2

OTHER IMPORTANT SECURITY MEASURES

Good job taking essential steps to improve your privacy in Chapter 1! It's important not to get discouraged by the fact that there is still a lot to do to protect your privacy. Remember that every step you take is a step closer to being protected online!

In this chapter, you will:

- ✓ Review the lessons learned in Chapter 2 of Privacy Crisis
- ✓ Identify the biggest privacy threats you create through your online activity
- ✓ Make a prioritized action plan for your next steps

You might remember an analogy in Chapter 1: “Security is locking your windows; privacy is covering them with blinds.” Well, if the things you did in Chapter 1 of this workbook was locking your windows, the tasks in Chapter 2 are about adding the security system, reinforcing your windows, replacing the locks, and building a safe room.

There are 14 different recommended actions in Chapter 2:

1. **Avoid Chinese Devices, Apps, and Services**
2. **Secure Your Data Transfers**
3. **Always Use a Virtual Private Network (VPN)**
4. **Lock Down Your Wireless Networks**
5. **Remove All Publicly-Viewable CVs or Resumes**
6. **Purge and Configure Your Google Account**
7. **Cleanse and Lock-Down Social Media Accounts**
8. **Migrate From "Free" Services to Privacy-Focused Alternatives**
9. **Change Your Mailing Address to a Post Office Box**
10. **Remove Personal Information From Your Domain Registration**
11. **Revoke Unnecessary Location Sharing**
12. **Use Dummy Information**
13. **Protect the Vulnerable**
14. **Maintain Vigilance**

You don’t have to do *all* of these things right now, but you should do them soon. If you don’t, you’re at risk from bad actors, including thieves, hackers, marketers, and people pushing disinformation.

After reading Chapter 2, you should prioritize some conscious choices about the digital services and providers you use on a daily basis.
The goal here is to set up long-term habits. For this to work, these
new privacy practices have to be sustainable and consistent.
This won’t work if you cheat!

ACTIVITY 1

CONDUCT A PERSONAL HABIT THREAT ANALYSIS

How risky are your online behaviors? For each item in the list below, rate your behavior on a scale of 0-3.

0=I never do this
1= I rarely do this
2=I sometimes do this
3=I frequently or always do this

Digital Behaviors:

- ___ Using free email services
- ___ Keeping old resumes/CVs online
- ___ Using the same password on multiple sites
- ___ Clicking through to websites from emails
- ___ Using public WiFi without a VPN
- ___ Allowing apps to access your location
- ___ Using Chinese-made apps/devices
- ___ Using 'free' services that collect your data
- ___ Using browsers without privacy protection
- ___ Storing sensitive files in cloud storage

Social Sharing Behaviors:

- ___ Posting about your travel plans
- ___ Sharing your work details online
- ___ Using your real name on forums/games
- ___ Participating in online surveys
- ___ Joining loyalty/rewards programs
- ___ Using social media check-ins
- ___ Sharing photos with location data
- ___ Using your real birthdate on accounts
- ___ Connecting with unknown people
- ___ Posting about valuable possessions

List your 5 highest-scored items in the left-hand column of the table below.

Then, answer the questions in the next columns. If you don't know the answers, refer to the section in Chapter 2 of *Privacy Crisis* that explores this concern.

(If you answered "3" to more than 5 behaviors, that's okay! We'll work on fixing those in Activity #2.)

High-Risk Behavior	What specific risks does this create?	Who could potentially exploit this?	What is the worst-case outcome of this behavior?	What's one step I could take to reduce this risk?
Example: Using Public WiFi Without a VPN	Anyone on the same network can intercept your data Login credentials could be captured Financial transactions could be monitored Personal communications could be intercepted Device could be directly attacked by others on the network	Hackers at coffee shops/airports Identity thieves targeting public spaces Cyber criminals running fake WiFi networks Corporate spies gathering business data Automated hacking tools running on public networks	Bank account compromised Email/social media accounts hijacked Work/business data stolen Identity theft Device infected with malware	Install and always use a reputable VPN service before connecting to any public WiFi
1				
2				
3				
4				
5				

ACTIVITY 2

MAKE A PRIORITIZED ACTION PLAN

Your last activity for **Chapter 2** is to make an action plan! With so many things to do, it can be overwhelming. Let's create an action plan so that you can stop feeling overwhelmed and start feeling empowered to take back control of your privacy.

Using the risk assessment from **Activity #1,** list the activities you do and put them in order from riskiest to least risky. This will help you prioritize the actions you need to take first vs. those you can work on later.

Based on the information you learned in **Chapter 2**, you get to decide which actions are riskiest and least risky. This list will be unique to every individual, because we all do activities differently. A small risk that you take every single day may be higher on your list than a large risk that you take only rarely.

In **Activity #1**, you already identified 5 of the biggest threats to your online security—this will help you figure out what you want to do after you've taken care of those five critical threats.

Most risky

1:

2:

3:

4:

5:

6:

7:

8:

9:

10:

11:

12:

13:

14:

15:

16:

17:

18:

19:

20:

Less risky

Using free email services

Keeping old resumes/CVs online

Using the same password on multiple sites

Clicking through to websites from emails

Using public WiFi without a VPN

Allowing apps to access your location

Using Chinese-made apps/devices

Using 'free' services that collect your data

Using browsers without privacy protection

Storing sensitive files in cloud storage

Posting about your travel plans

Sharing your work details online

Using your real name on forums/games

Participating in online surveys

Joining loyalty/rewards programs

Using social media check-ins

Sharing photos with location data

Using your real birthdate on accounts

Connecting with unknown people

Posting about valuable possessions

! Now you know what you need to focus on first!

CHAPTER 3

THE SCOPE, HIERARCHY, AND VALUE OF PERSONAL DATA

Chapter 3 of Privacy Crisis walks you through three important categories of personal information.

1. **Public information** is accessible to anyone through ordinary means. If someone could look up this information in a phone directory, from public records, or what they have observed about you in public spaces, then it's public. Despite being visible to the public, you should still do your best to avoid carelessly adding information to the public sphere.

2. **Private information** isn't necessarily secret, but you would likely prefer that it stays within your inner circle of family and friends. This category includes your date of birth, phone number, employment history, physical description, and personal interests or hobbies. Even though this information is not strictly confidential, it can be used for problematic purposes when it is collected and analyzed.

3. **Secret information** should remain strictly confidential. This data includes your Social Security number, financial history, passwords, health information, and anything that could cause harm if exposed. This information should never be shared, except in circumstances when it is absolutely necessary.

Understanding these categories helps you make informed decisions about what information to share, with whom, and under what circumstances.

As you work through these activities, you'll develop a clearer picture of your own information landscape and create strategies to better protect your digital identity.In this workbook chapter, you will:

- Understand the 3 types of personal data (Public, Private, and Secret)
- Learn about who currently has access to your personal data
- Create a data breach scenario to recognize what steps you need to take to protect your data

ACTIVITY 1

UNDERSTANDING WHO HAS ACCESS TO YOUR PERSONAL DATA

The goal of this activity is to help you visualize which entities currently have access to your personal information.

Below, you'll find two tables.

In table #1, you'll see examples of types of data, divided into our three color-coded groups (Public, Private, and Secret).

Table 1

Public Data	Private Data	Secret Data
Full name Voter registration status and party affiliation Public records (court cases, real estate transactions, liens, judgments) Details revealed in news stories Charitable and political donations Military service records Vehicle license plate numbers	Age and date of birth Race/ethnicity/citizenship status Marital or relationship status Gender/sexual orientation Personal cell phone number Current and previous home addresses IP address Device MAC addresses	Social security number Bank account details Credit card numbers Account information for services you use Insurance policy details Login credentials and passwords PINs DNA/genetic data Information about addictions

Public Data	Private Data	Secret Data
	Online aliases (usernames, player IDs, handles) Physical description (weight, height, hair color, tattoos, scars, disabilities) Work contact information Current and past employment Driving record Private health information Academic records Relationship history Names of current and former pets Annual household income Credit score and history Internet and mobile service providers Purchase history Personal preferences and brand loyalties Languages spoken	Information kept secret from spouse, children, or employer Any information that would harm your life, career, or relationships if revealed

Table 2

In table #2, you'll see a list of organizations, institutions, and individuals. Under each category, identify which categories of data each organization has access to. For example, almost all of the categories may have access to your date of birth. However, only a handful should have your personal health data.

Place each piece of data from Table #1 and place it in every category on this table. Most likely, each piece of data will appear in multiple locations.

Government Agencies	Financial Institutions	Healthcare Providers	Tech Companies	Retailers & Loyalty Programs	Social Media	Employers and/or Schools

Next step: Color code each piece of data you placed on the table, according to whether it is Personal, Private, or Secret.

We recommend using a stoplight approach:

🟢 Personal Data (Green)	🟡 Private Data (Yellow)	🔴 Secret Data (Red or Orange)

1. **Which group/organization has the most information about you?**

2. **Which categories concern you the most?**

3. **Are there any surprises in your answers?**

ACTIVITY 2

DATA BREACH SIMULATION

Next, we are going to simulate a data breach and practice navigating the process of responding to it.

Step 1

Choose one of the categories from Table 2 in the previous activity (government agencies, financial institutions, etc.)

Now, imagine that this organization had a data breach. For example, you could imagine that your healthcare provider had a data breach.

What category did you choose?

Step 2

Circle a hypothetical scenario below to use for the rest of the activity.

- Your email account and password were accessed by a disgruntled employee
- Your Social Security Number was accessed in a data breach
- An employee was tricked by a social engineering scam and surrendered your private data to a cybercriminal
- Employee error led to accidental data exposure (emails sent to wrong recipients, files improperly shared)
- Database security vulnerability allowed unauthorized access to customer records
- A third-party vendor with access to your data was compromised
- Software update/patch was not applied, allowing known security vulnerabilities to be exploited
- Malware infection compromised network security and allowed data exfiltration

Step 3

Based on Table 2 in the previous activity, list 5 pieces of your personal information that might be exposed in this breach

1. ______________________________
2. ______________________________
3. ______________________________
4. ______________________________
5. ______________________________

Step 4

Based on Table 2 in the previous activity, list 5 pieces of your personal information that might be exposed in this breach

Check all that could happen because of this breach:

□ Spam emails
□ Identity theft
□ Financial loss
□ Account takeovers
□ Embarrassing information exposed
□ Phishing attempts
□ Reputation damage
□ Other: _________________

Step 5

Based on Table 2 in the previous activity, list 5 pieces of your personal information that might be exposed in this breach

1. ______________________________
2. ______________________________
3. ______________________________

Step 6

What could you do to make sure your data is not compromised if this organization experiences a breach of some kind? Select as many as apply.

□ Provide only the minimum required information when creating accounts

□ Use a unique, strong password for this organization's accounts

□ Enable two-factor authentication if available

□ Use a masked or temporary email address for this organization

□ Monitor accounts regularly for suspicious activity

□ Opt out of unnecessary data sharing with "partners"

□ Use a P.O. box instead of home address when possible

□ Use a password manager to generate and store credentials

□ Request a copy of what data they store about you

□ Request deletion of unnecessary personal data they hold

□ Review and update privacy settings regularly

□ Sign up for breach notifications from the organization

□ Use a credit freeze to prevent unauthorized accounts

□ Use a virtual credit card number for online payments

□ Create a system for identifying legitimate communications from the organization

□ Avoid using social media logins to access the organization's services

□ Encrypt sensitive documents before sharing them

□ Check if the organization offers privacy tools or opt-out options

□ Use secure communication methods when sharing sensitive information

□ Read privacy policies to understand how your data is used and protected

□ Request your data be stored only for the minimum time necessary

CHAPTER 4

THE DIRECT CONSEQUENCES OF SURRENDERING YOUR DATA

Chapter 4 of *Privacy Crisis* explores the immediate and tangible consequences that can occur when your personal information falls into the wrong hands. While previous chapters focused on categorizing your data and understanding how it's collected, this chapter examines what actually happens when privacy is compromised!

The chapter covers two main categories of harm: virtual/electronic harm and real-world physical harm.

- **Digital harm:** When your compromised personal information leads to identity fraud, financial theft, account takeovers, extortion, ransomware attacks, and various forms of spam

- **Physical harm:** When your leaked personal data enables swatting, robbery, vandalism, harassment, and legal problems.

The chapter emphasizes that privacy breaches aren't merely inconveniences—they can cause profound financial loss, psychological trauma, reputation damage, and even physical danger. Through powerful case studies like the Wells Fargo fraudulent accounts scandal, the Ashley Madison data breach, and accusations of being a terrorist levied at innocent people, Chapter 4 illustrates how corporate negligence and malicious actors can devastate individuals' lives.

In this workbook chapter, you will:

- Take note of the data breaches that you and those you know have experienced (Privacy Breach Bingo)
- Consider the real-world and digital risks of a privacy breach
- Take a short “What Would You Do?” quiz to test your knowledge of the best steps to take after a breach

By understanding these direct consequences, you'll be better equipped to make informed decisions about what information you share and with whom you share it. The activities in this workbook section will help you prepare for possible privacy breaches and create action plans to protect yourself from the most common and damaging scenarios.

ACTIVITY 1

PRIVACY BREACH BINGO

Mark each square if you or someone you know has experienced it:

Doxxing	Personal info found online	Unauthorized account created	Junk mail from data brokers	Strange charges on accounts
Computer virus or malware	Scam text messages	Banking fraud	Fake account in your name	Social media impersonation
SIM-jacking	Ransomware attack	**FREE SQUARE**	Data breach notification	Targeted ads following you
Email account compromised	Password stolen	Online account locked	Phishing attempt	Identity theft
Stalking or harassment	Credit card fraud	Social media account hacked	Unwanted phone calls	Spam email bombardment

Follow-up questions:

1. How many squares did you mark off?
2. Which ones surprised you?
3. Which unmarked square concerns you most?

Create a plan:

In the space below, write 3 steps you can take to prevent one of the signs of a breach from happening again. You can use earlier chapters of Privacy Crisis to find ideas for how to prevent this from happening (or happening again!).

ACTIVITY 2

DIGITAL BREACHES WITH REAL-WORLD CONSEQUENCES

Below you will find several potential privacy breach scenarios. For each one, check the real-world consequences that could happen—you may check one or more under each breach. Then, determine which one you think is most likely.

Here's an example:

Digital Breach: Your fitness app location data is accessed

Possible Real-World Consequences:

- [✓] Home burglary when thieves see you're not home
- [✓] Stalking based on your regular running routes
- Identity theft
- Credit card fraud
- [✓] Harassment at locations you frequently visit
- **Most likely:** Home burglary when thieves see you're not home

Here are the potential breaches:

Digital Breach: Your home address and vacation dates are posted online

Possible Real-World Consequences:

- Home burglary
- Package theft
- Stalking
- Swatting
- Harassment at home
- **Most likely:** ____________________________________

Digital Breach: Your financial information has been stolen

Possible Real-World Consequences:

- Empty bank accounts
- New accounts opened in your name
- Creditors are calling you about debts you didn't create
- Denied loans or housing
- Tax return fraud
- **Most likely:** ______________________________

Digital Breach: Your work history and employer are exposed

Possible Real-World Consequences:

- Workplace harassment
- Being targeted for corporate espionage
- Social engineering attacks on your colleagues
- Job discrimination
- Targeted scams related to your industry
- **Most likely:** ______________________________

Digital Breach: Your personal photos are accessed

Possible Real-World Consequences:

- Blackmail attempts
- Public embarrassment
- Fake profiles using your image
- Damaged relationships
- Deepfake videos created with your likeness
- **Most likely:** ______________________________

Digital Breach: Your shopping history is sold to data brokers

Possible Real-World Consequences:

- Higher prices when shopping online
- Targeted by scams related to products you buy
- Receiving unwanted physical mail and packages
- Insurance rate increases based on purchases
- Judgments about lifestyle from employers/others
- **Most likely:** ______________________________

Reflect on these possible scenarios.

1. Which scenario concerns you the most? Why?

2. Did any of the connections between digital breaches and real-world consequences surprise you?

3. What's one action you could take today to prevent your most concerning scenario?

ACTIVITY 3

"WHAT WOULD YOU DO?" QUIZ

For each scenario, circle what you would do first:

1. You receive a notification that your email password was changed, but you didn't change it.

Try to log in with your old password

Contact the email provider immediately

Check if other accounts are compromised

Ignore it—probably just a glitch

2. Your credit card shows charges you didn't make.

Try to log in with your old password

Contact the email provider immediately

Check if other accounts are compromised

Ignore it—probably just a glitch

3. You receive an email claiming to have embarrassing videos of you.

Pay what they're asking to keep it private

Reply and ask for proof

Ignore it—it's likely a scam

Contact the police

4. Someone posts your home address on social media.

Ask them to remove it immediately

Report it to the platform

Consider staying somewhere else temporarily

Dismiss it as not important

5. You discover your child is being tracked through a gaming app.

Delete the app immediately

Contact the app developer

Disable location services for all apps

Report to authorities

See the correct answers below!

Correct answers for “What Would You Do?” Quiz

1. **You receive a notification that your email password was changed, but you didn't change it.**

   Correct answer: B) Contact the email provider immediately

   Here’s why: Immediate contact with the email provider allows them to freeze the account, prevent further unauthorized access, and begin the account recovery process before more damage can be done.

2. **Your credit card shows charges you didn't make.**

   Correct answer: A) Call the credit card company immediately

   Here’s why: Immediate notification to your credit card company allows them to stop fraudulent charges, cancel the compromised card, issue a new one, and initiate their fraud investigation process to protect you from liability.

3. You receive an email claiming to have embarrassing videos of you.

Correct answer: C) Ignore it—it's likely a scam

Here's why: These emails are typically mass-sent scams with no actual compromising material, and responding or paying only confirms your email is active and makes you a target for additional scams.

4. Someone posts your home address on social media.

Correct answer: B) Report it to the platform

5. You discover your child is being tracked through a gaming app.

Correct answer: C) Disable location services for all apps

CHAPTER 5

THE INDIRECT CONSEQUENCES OF SURRENDERING YOUR DATA

Our previous chapters focused on immediate threats like identity theft or account hacking, Chapter 5 explores something more subtle but equally dangerous: how your personal data is used to influence your behavior without your knowledge. Every time you browse, click, or engage online, sophisticated algorithms collect information about your interests, habits, and vulnerabilities. This isn’t just because they want to understand you; they also want to change you!

This chapter's activities help you recognize the invisible forces shaping your decisions. In this chapter, you will:

- Analyze your purchasing habits to see how target marketing affects your spending
- Identify manipulation techniques you have experienced recently
- Conduct an experiment to see how your algorithm is shaped by your online activities

The goal isn't to make you paranoid about technology, but to help you become more conscious of how your data is being used against you. Once you know how these forces can influence you, you can start making more intentional choices about your digital life rather than being subtly directed by companies that profit from your attention and spending. Remember: the most dangerous manipulation is the kind you don't notice happening.

ACTIVITY 1

ANALYZE YOUR UNPLANNED PURCHASES

Chapter 5 discusses how hard corporations work to get your money. The more data they have on you, the more effectively they can target you to buy their products and services.

To evaluate how successful they are, think about your most recent unplanned purchases. This includes anything you bought that wasn't already on a shopping list or something you needed to purchase.

For each item, consider how you learned about it.

Item	Price	How did you learn about it?
	$	☐ Ad ☐ Social media post ☐ Friend or family member ☐ Store display ☐ Other: _____________
	$	☐ Ad ☐ Social media post ☐ Friend or family member ☐ Store display ☐ Other: _____________

Item	Price	How did you learn about it?
	$	□ Ad □ Social media post □ Friend or family member □ Store display □ Other: _____________
	$	□ Ad □ Social media post □ Friend or family member □ Store display □ Other: _____________
	$	□ Ad □ Social media post □ Friend or family member □ Store display □ Other: _____________
	Total spent on unplanned purchases: $	

Analysis questions

1. How many of these purchases were influenced by targeted marketing (marketing based on the vendor's knowledge of you and/or your spending habits)?

2. Do you have any regrets about these purchases? Why or why not?

3. Would you have bought this item if the marketer had not been able to target you directly?

ACTIVITY 2

IDENTIFY MANIPULATIVE BEHAVIORS FROM MARKETERS

Chapter 5 of *Privacy Crisis* addresses the fact that marketers, retailers, media producers, lobbyists, and more will often try to manipulate you into feeling certain things because those feelings can lead to spending.

To understand how commonplace this manipulative behavior is, check any of the boxes that you have experienced in the last 2 weeks:

□ Found yourself spending more time on an app than you intended

□ Bought something you hadn't planned to buy

□ Felt angry after reading news or social media content

□ Noticed your opinions becoming stronger on political topics

□ Felt inadequate after seeing social media content

□ Received "personalized" offers that seem to know what you want

□ Found that certain content keeps appearing in your feed

□ Experienced FOMO (fear of missing out) when seeing others' activities

□ Got notifications designed to pull you back to an app

□ Shown increasingly extreme content on topics you've shown interest in

□ Felt compelled to "grind" or complete tasks in a game even though it wasn't enjoyable

□ Found yourself buying something just because it was on "sale"

□ Made a purchase due to a limited-time offer, creating urgency

□ Felt anxious when you couldn't check your social media

□ Found yourself comparing your life unfavorably to others online

- □ Been presented with content that confirms beliefs you already hold
- □ Received emails about items left in your online shopping cart
- □ Found yourself doom-scrolling through negative news or content
- □ Noticed recommended videos becoming increasingly addictive
- □ Felt pressured to participate in trending topics or challenges
- □ Been bombarded with ads after researching a product once

If you checked off several boxes, you're experiencing what the book calls "indirect consequences" of surrendering your data. These aren't accidents - they're deliberate strategies designed to influence your behavior.

The more boxes you checked, the more successful these manipulation techniques have been in your life. This doesn't mean you're weak-willed; these systems are scientifically engineered to exploit human psychology, and they work on almost everyone.

What to do with this information:

1. Recognize the pattern

2. Reclaim your attention (Consider using screen time limits, turning off notifications, or scheduling specific times to check social media rather than responding to every alert)

3. Practice mindful consumption by waiting to make purchases

4. Diversify your information sources (Seek viewpoints from outside of your algorithm)

5. Value your data

Remember: The goal isn't to completely disconnect from technology, but to use it intentionally rather than letting it use you. By understanding these manipulation techniques, you can make more conscious choices about your attention, time, and spending.

ACTIVITY 3

TEST YOUR ALGORITHM

This last activity for Chapter 5 is to test your personal algorithm. Let's find out how your online behaviors affect the information, ads, and offers you receive when you're browsing the internet or social media.

This activity will take a week to complete. You can continue the workbook while you complete this activity, which will let you experience firsthand how algorithms adapt to your behavior and create online bubbles that are hard to break out of.

Part 1: Setup

1. Choose one social media platform or search engine to experiment with

2. For 2-3 days, use the platform normally without changes

3. What kinds of ads do you see? How often do you want to buy something from those ads?

Part 2: Intervention

1. For the next 3-4 days, deliberately interact with content on a specific topic you normally don't engage with (choose something neutral like "hiking," "baking," or "classic cars")

2. Like, click, view, or search for this topic several times each day

3. Do NOT change any other browsing habits

Part 3: Analysis

1. Document how quickly the algorithm began showing you more content related to your new topic

2. Note any ads that appeared related to this topic

3. Observe how the content changed over time (more specific, more extreme, etc.)

4. Document how long the effect lasted after you stopped engaging with the topic

Questions for Analysis:

How quickly did the algorithm adapt to your new interest?

How persistent was the change to your feed/results?

What types of content did the algorithm assume you'd like based on this interest?

What products or services were you shown ads for?

How might this effect impact someone's worldview if applied to important content, like politics, social issues, and health information, religious beliefs, and scientific understanding?

CHAPTER 6

OPTING OUT AND LOCKING DOWN

Chapter 6 of *Privacy Crisis* focuses on practical strategies to reclaim your privacy by opting out of data collection, locking down your accounts, and removing personal information that's already out there.

While total privacy may be impossible in the digital age, this chapter provides actionable steps to significantly reduce your information footprint and minimize future data collection. The following activities will help you implement these critical privacy protections and take back control of your personal information.

In this chapter, you will:

- Conduct a data breach check to find out where your information may have been accessed without your consent
- Perform a social media cleanse to remove personal information from some of the most popular social media platforms

ACTIVITY 1

CONDUCT A DATA BREACH CHECK

Let's discover which, if any, of your accounts have already been compromised.

WhatIsMyIPAddress.com offers a free data breach check at this page: https://whatismyipaddress.com/breach-check

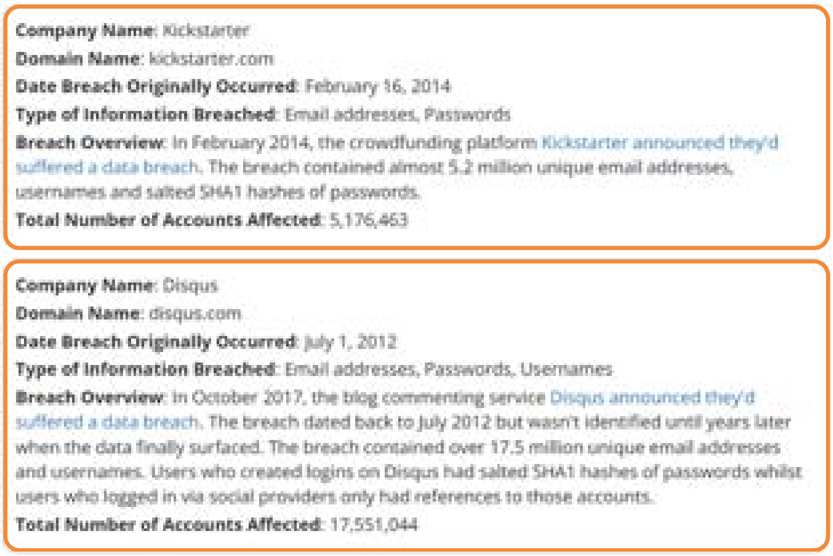
All you have to do is input your email address and review the results. This is what you'll see if your email address is in the clear and has never been part of a data breach

Breach Status

Congratulations! This email address has not been found in any data breaches!

All breach data sourced from haveibeenowned.com

However, if you have used your email for a while, you are more likely to see results like this:



Company Name: Kickstarter
Domain Name: kickstarter.com
Date Breach Originally Occurred: February 16, 2014
Type of Information Breached: Email addresses, Passwords
Breach Overview: In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.
Total Number of Accounts Affected: 5,176,463

Company Name: Disqus
Domain Name: disqus.com
Date Breach Originally Occurred: July 1, 2012
Type of Information Breached: Email addresses, Passwords, Usernames
Breach Overview: In October 2017, the blog commenting service Disqus announced they'd suffered a data breach. The breach dated back to July 2012 but wasn't identified until years later when the data finally surfaced. The breach contained over 17.5 million unique email addresses and usernames. Users who created logins on Disqus had salted SHA1 hashes of passwords whilst users who logged in via social providers only had references to those accounts.
Total Number of Accounts Affected: 17,551,044

Make a list below of any sites and platforms where your email, password, or other data may have been breached.

For any account still active on a breached service, change the password immediately. If you've reused that password elsewhere, change those accounts, too. Wherever possible, enable two-factor authentication.

ACTIVITY 2

UNDERGO A SOCIAL MEDIA CLEANSE

Chapter 6 explains the importance of opting out of activities that share your information online. Social media has its benefits, but the data security risks outweigh those benefits for many people. If you want to stay connected with people via social media for personal or professional reasons, you can still remove sensitive information from these accounts.

For each platform you use, go through this privacy cleanup checklist:

Facebook

□ Review and restrict the audience for past posts

□ Remove personal information from profile (DOB, relationship status, etc.)

□ Review and limit app connections

□ Download your data before deleting content

□ Remove location data from posts

□ Review tagged photos and remove tags

□ Create a pseudonym or limit searchability

□ Opt-out of ad targeting

Twitter/X

□ Audit old tweets for personal information

□ Delete problematic tweets or use the auto-delete service

□ Restrict who can tag you

□ Turn off location sharing

□ Review third-party app connections

□ Control discoverability settings

□ Opt-out of personalization

LinkedIn

□ Review what's visible to the public vs. connections

□ Limit profile details to professional information only

□ Turn off "notify network" for profile changes

□ Control connection requests

□ Review third-party application access

□ Manage who can see your connections

LinkedIn

□ Make the account private

□ Review and remove location tags from posts

□ Manage tagged photos

□ Review story highlights for personal information

□ Control who can mention you

□ Limit account access by third-party apps

When reviewing and removing your personal info from these sites, what information were you most surprised to find publicly available about yourself?

What was the most difficult type of information to remove?

CHAPTER 7

THE HIDDEN COSTS OF PRIVACY

In Chapter 7 of Privacy Crisis, you learned about the challenges and obstacles you may face when you decide to protect your privacy. Ultimately, the internet is designed to get you to hand over your information, and a lot of sites are difficult to interact with if you are taking privacy precautions.

The following activities will help you recognize, navigate, and overcome these hurdles.

In this workbook chapter, you will:

- Conduct a cost-benefit analysis, comparing privacy and convenience

- Practice what to say or do when you're confronted with a challenge to your privacy

ACTIVITY 1

COST-BENEFIT ANALYSIS OF PRIVACY VS. CONVENIENCE

Let's explore some of the convenience tradeoffs that come with protecting your privacy. For each of the items in the table below, you're going to answer 4 questions:

- What are the costs of privacy?
- What are the benefits of privacy?
- Is it worth it to you to have privacy in this area?
- Is there an alternative available to you?

We'll fill out the first one, and you can do the rest.

Item	Privacy Cost	Benefits to You	Worth It? (Y/N)	Alternative?
Store loyalty card	Tracks all purchases, ties them to your identity, sells data to partners	5-10% discounts on select items, occasional personalized coupons	No	Use cash; use privacy-focused alternatives like temporary /masked phone numbers for signup
Voice assistant (Alexa, Google, Siri, etc.)				

Item	Privacy Cost	Benefits to You	Worth It? (Y/N)	Alternative?
Social media account				
Free email service				
Food delivery app				
Smart TV features				
Add your own:				
Add your own:				
Add your own:				

ACTIVITY 2

PREP FOR THE PRIVACY GAUNTLET

Once you start protecting your privacy, you also start facing challenges to it. In Chapter 7, you learned about some of the challenges you may face after you stop allowing organizations, businesses, and other entities to access your personal information. In this activity, you will prepare for these encounters by developing an action plan.

Write down your plan for each of the following challenges below. When you're in the gauntlet of protecting your privacy, you can fall back on these practiced responses. Use the information in Chapter 7 of Privacy Crisis to make your plans.

Scenario: Someone says, "We need to see your ID for security purposes."

Scenario: You are on the phone with a company, and they say, "Our website doesn't work with VPNs, so you will need to turn off your VPN to use our site."

Scenario: You encounter an app that says, “This feature requires location access.”

Scenario: You are trying to use an app or website, but it says, “You must create an account to continue.”

Scenario: You are prompted to “Enter your phone number for verification.”

Sample Answers for Privacy Gauntlet Prep

Scenario: Someone says, "We need to see your ID for security purposes."

I will:

- Ask what specific information they need to verify and why.
- If showing ID is necessary, I'll say: "I'm happy to show you my ID for verification purposes, but I don't consent to it being photographed or copied. If you need to record that you've verified my identity, please just note that ID was presented."
- If they insist on copying, I'll ask to speak with a manager to discuss alternatives or consider whether the service is worth this privacy tradeoff.

Scenario: You are on the phone with a company, and they say, "Our website doesn't work with VPNs, so you will need to turn off your VPN to use our site."

I will say, "I understand your security concerns, but I use a VPN to protect my personal information. Can you explain exactly what functionality is limited? If it's just for account creation, I might temporarily disable it for that specific purpose only. Otherwise, I'll need to explore companies that offer similar services without restricting privacy tools."

Scenario: You encounter an app that says, "This feature requires location access."

- Check if the app offers the option to use location 'only while using the app' rather than always.
- If the feature truly requires location, I'll determine if it's essential to my use of the app. If not, I'll skip that feature.
- If location is required for core functionality, I'll consider whether the service's value justifies the privacy tradeoff.
- For map apps or delivery services where location makes sense, I'll grant temporary permission only.

Scenario: You are trying to use an app or website, but it says, "You must create an account to continue."

- I’ll look for a 'continue as guest' option first.
- If that's not available, I'll evaluate whether this is a service I'll use frequently enough to justify creating an account. If I decide to create one, I'll use a masked email address, a unique password from my password manager, and provide only the minimum required information.
- For one-time purchases, I'll consider whether there are alternative sites that don't require accounts.

Scenario: You are prompted to "Enter your phone number for verification."

- I'll first check if there are alternative verification methods like email.
- If phone verification is required, I'll consider using a secondary phone number service like Google Voice rather than my primary number.
- For services that aren't essential, I'll evaluate whether the requirement for my phone number outweighs the benefit of using the service.
- I'll also check their privacy policy to see how they plan to use and protect my phone number.

CHAPTER 8

HOW TO BE FOUND (THE “RIGHT WAY”)

Chapter 8 of *Privacy Crisis* explores the balance between maintaining privacy while still being discoverable by the right people in the right contexts. This chapter acknowledges that most people do want to be found by certain audiences, so let’s use some strategies that allow you to be selectively visible—without compromising your overall privacy and security.

The following activities will help you implement these strategies to maintain a deliberate, controlled online presence while protecting your personal information.

In this workbook chapter, you will:

- Design a strategy for when and where to use a pseudonym
- Create a selective disclosure framework
- Establish clear boundaries between personal and professional identities

ACTIVITY 1

DESIGN YOUR PSEUDONYM STRATEGY

Chapter 8 discusses a privacy-focused strategy of using pseudonyms or professional names as a way to create separation between your public and private identities. In this activity, you will create your own pseudonym plan, which you can implement.

Step 1:
Here is a list of commonly used websites where you might have used your first, last, or full name. You may need to double-check, especially if you haven't used these sites in a while. However, if you have used any part of your name for these accounts, either as the username or public-facing account handle, circle the site on the list.

LinkedIn
Facebook
Twitter/X
Instagram
YouTube
Medium
Substack
Reddit
Pinterest
Quora
GitHub
Stack Overflow
SlideShare
Academia.edu
ResearchGate
Behance
Dribbble

DeviantArt
Etsy
eBay
Amazon (reviews and seller profiles)
Goodreads
Yelp
TripAdvisor
Meetup
Nextdoor
WhatsApp
Telegram
Discord
Twitch
Patreon
Ko-fi
Threads

Mastodon
Bluesky
TikTok
Snapchat
Tumblr
WordPress blogs
Blogger/Blogspot
Flickr
500px
Vimeo
SoundCloud
Spotify (public playlists)
Airbnb
HomeAway/VRBO
Fiverr
Upwork
Thumbtack

Step 2:
Decide which sites need to be changed. It's always a good idea to delete accounts on sites you no longer use, and that's even more important if your name is anywhere on the account.

On some of these sites, you may decide it's worth it to keep your name attached. LinkedIn is an example of a site where lots of people use their full name.

Step 3:
Choose a pseudonym. If you need to use a first and last name on some of these sites, consider using a pseudonym. It should:

- Reflect your professional identity
- Be memorable
- Not directly connected to your personal identity

Potential names (list 3-5):

-
-
-
-
-

Step 4:
Check the availability of this name against multiple platforms, including domain names, social media handles, email addresses, etc.

Consider this: Privacy Crisis mentions that if you use a pseudonym or professional name, you should use it consistently across professional platforms to maintain a cohesive online presence.

ACTIVITY 2

CREATE A SELECTIVE DISCLOSURE FRAMEWORK

Let’s consider which information you share with different audiences! After all, there are times when you want to be discovered online.

Identify what information you're comfortable sharing with each group by checking the appropriate boxes:

Information Type	Close Friends & Family	Professional Contacts	Public Internet
Full legal name	□	□	□
Date of birth	□	□	□
Home address	□	□	□
Personal phone number	□	□	□
Work phone number	□	□	□
Personal email	□	□	□
Professional email	□	□	□
Current employer	□	□	□
Job title	□	□	□
Employment history	□	□	□
Education history	□	□	□
Social media profiles	□	□	□
Family members' names	□	□	□
Personal photos	□	□	□
Professional photos	□	□	□
Hobbies/interests	□	□	□

Use this information to set 3 rules for yourself. For example, your rules might be:

- I will always think twice before I share my personal information with someone who might not need it.
- I will only share my family members' names with people who absolutely need it.
- I will never post my personal photos on the public internet.

What are your rules?

1. ____________________

2. ____________________

3. ____________________

CHAPTER 9

THE ENSHRINEMENT AND FUTURE OF DATA RIGHTS

Chapter 9 of *Privacy Crisis* explores how we can move beyond individual privacy protection to help establish and defend data rights on a broader scale. This is incredibly important if we want to put a stop to the constant threats against our privacy.

This chapter examines how to advocate for privacy, including supporting organizations fighting for data rights, making ethical consumer choices, and preparing for future privacy challenges.

The following activities will help you become an advocate for privacy rights and contribute to a future where personal data is better protected.

In this workbook chapter, you will:

- Evaluate companies based on their privacy practices
- Support organizations working for data rights
- Reflect on Privacy Crisis and the activities you've included in this workbook

ACTIVITY 1

RATE THE PRIVACY PRACTICES OF COMPANIES YOU USE

Chapter 9 encourages "rewarding the virtuous and shunning the wicked" when it comes to companies' data practices.

Step 1:
List five companies or services you regularly use. These can be your go-to brands, your favorite place to shop, or the social media platforms you use the most.

1. ______________________________

2. ______________________________

3. ______________________________

4. ______________________________

5. ______________________________

Step 2:

Rate each company's privacy practices by researching their policies and history:

Name of Company	Does the company have a clear privacy policy on their website? Yes=1 point No = 0 points	Google the company name + "Data breach" No data breaches = 1 point Data breaches in their history = 0 points	Find out if they allow you to opt out of data collection while using their services Yes, they allow you to opt-out = 1 point No, you can't opt out = 0 points	Find out if the company sells your data to data brokers. No, they don't sell to data brokers = 1 point Yes, they sell to data brokers = 0 points	Total ranking (0-4)

Step 3:
For any company scoring below 3, list potential alternatives. You will need to look into the privacy practices of those companies before making a change.

Current Company	Potential Alternatives

Step 4:
There is one last step for this activity! In order to draw more attention to the problem of privacy, consider this: If you decide to stop spending your money with one of your favorite companies because of their poor privacy choices, send an email to the company (maybe even to the CEO) about your decision. Don't just disappear. Let them know why you're leaving!

ACTIVITY 2

SUPPORT PRIVACY ORGANIZATIONS

Chapter 9 mentions several organizations fighting for privacy and data rights that deserve support:

- Electronic Frontier Foundation (EFF)
- Mozilla Foundation
- American Civil Liberties Union (ACLU)

Spend some time researching these organizations and choose at least one to support.

□ Make a donation

□ Sign up for their newsletter

□ Share their resources on social media

□ Use their privacy tools

□ Volunteer time or skills

□ Other: ____

ACTIVITY 3

REFLECT ON YOUR PRIVACY JOURNEY

Congratulations on completing the *Privacy Crisis* workbook!

Over the last 9 chapters, you have taken important steps toward protecting your personal information and reclaiming your privacy. This final exercise helps you reflect on what you've learned, how your perspective has changed, and the impact these changes will have on your digital life moving forward.

Step 1:
What were the three most important or surprising things you learned from Privacy Crisis and this workbook?

1. ____
   ____
2. ____
   ____
3. ____
   ____

Step 2:
List 3-5 specific privacy actions you've already taken as a result of this workbook:

1. ____
   ____

2. ____________________

3. ____________________

4. ____________________

5. ____________________

Which change was the most challenging to implement? Why?

____

____

____

Which change do you think will have the biggest positive impact on your privacy? Why?

____

____

____

Step 3:
How has your thinking about privacy and personal data changed since beginning this workbook?

Before starting Privacy Crisis, I thought:

____

____

____

Now I believe:

Step 4:
Looking forward to the future

How will you stay informed about evolving privacy threats and protections?

Do you plan to share what you've learned with others? If so, how?

What is one thing you wish everyone knew about privacy and data rights?

Final Reflection

Complete this sentence: "Taking control of my privacy matters because..."

Remember: Privacy is an ongoing journey, not a destination. Technology will continue to evolve, and there will always be new challenges to learn about and respond to. The good news is that the skills and knowledge you've gained from Privacy Crisis will prepare you for a conscientious and attentive future. You are now making better, more informed decisions about your digital life!

PRIVACY CRISIS

NOW THAT YOU'VE DONE THIS

CONGRATULATIONS

YOU'VE TAKEN PRACTICAL STEPS TO PROTECT YOUR PRIVACY

Share it with a friend

CHRIS PARKER