National Data Privacy
Standards Manual

prima

National Data Privacy

Standards Manual

Designed by prima / Savannah 2022

Contents

The following pages of the Prima Data Privacy Standards Manual, listed in sequential order, are officially in effect as of June 2, 2022.

Dear American People:

A driving force and use of innovative strategies for protecting individuals' data privacy have brought Prima the image of a get-it-done agency, and the record backs up the reputation.

As we move ahead to an even more exciting era in data privacy research and exploration, we have added a new tool to enhance and symbolize the progressive path we believe should always be followed when monitoring personal safety.

We have adopted a new system of graphics — the visual communications system by which we are known to those who read our publications, see our digital presence and public displays and the logotype that unmistakably brands them as Prima's.

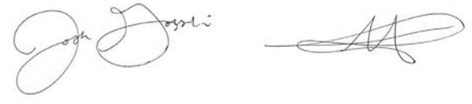
We believe this logotype presents Prima's utmost importance of our peoples' individual rights to privacy and the severity of this global crisis. Unity, preparation, pioneering change — that's what Prima is all about.

This manual is a reference book for the American people. It is the official policy document regarding data privacy identification, protection in general sets as well as specific targeted attacks, and level of quality for all personal data.

Our experience has shown that, in order to succeed, a program which departs from the accustomed must have the full support of all American people. Top-level management must take the lead, our experts in the field of data protection must follow, and all of us must see that the specifics are diligently monitored to insure that standards of excellence are maintained.

We think we were fortunate in recognizing that public communication could stand improvement; I am confident that the program we now have underway will be second to none in effectiveness either in government or industry; and we solicit the enthusiastic support of each of you in implementing personal data protection's look of the future.

Sincerely,



Josh Gorski and Michael Heathershaw
Administrators of Prima

Preface

We built this organization in the hopes of trying to unify the nation and diminish the level of fear and lack of trust regarding the mishandling of their personal data. We set out these standards as a guide to help every individual understand what exact rights they have and what all they can expect to see in the world moving at a mile a minute, right in front of their eyes.

We're at a time where it is the utmost duty to do whatever we can to unite the American people and bring back the idea of trust, and trust in one another. This data privacy standards manual is a guide for how every individual should maintain control over their lives and those around them that could also be impacted.

Here at Prima, our goal is to help assist you. We want you to feel safe and protected with the way you live your every day life and give you some starting points of where you can protect yourself and your information. In this manual we layout the general precautions to take as well what you can expect in a data breach, and what you can look for in avoiding having your privacy being taken. Whether it's a data breach, or just larger companies using too much of your information, there are ways you can keep yourself and your information safe.

For further details regarding how you can stay safe, visit us on our website at **primanual.com**

Dear American People:

A driving force and use of innovative strategies for protecting individuals' data privacy have brought Prima the image of a get-it-done agency, and the record backs up the reputation.

As we move ahead to an even more exciting era in data privacy research and exploration, we have added a new tool to enhance and symbolize the progressive path we believe should always be followed when monitoring personal safety.

We have adopted a new system of graphics — the visual communications system by which we are known to those who read our publications, see our digital presence and public displays and the logotype that unmistakably brands them as Prima's.

We believe this logotype presents Prima's utmost importance of our peoples' individual rights to privacy and the severity of this global crisis. Unity, preparation, pioneering change — that's what Prima is all about.

This manual is a reference book for the American people. It is the official policy document regarding data privacy identification, protection in general sets as well as specific targeted attacks, and level of quality for all personal data.

Our experience has shown that, in order to succeed, a program which departs from the accustomed must have the full support of all American people. Top-level management must take the lead, our experts in the field of data protection must follow, and all of us must see that the specifics are diligently monitored to insure that standards of excellence are maintained.

We think we were fortunate in recognizing that public communication could stand improvement; I am confident that the program we now have underway will be second to none in effectiveness either in government or industry; and we solicit the enthusiastic support of each of you in implementing personal data protection's look of the future.

Sincerely,

Josh Gorski and Michael Heathershaw
Administrators of Prima

prima

prima

prima

prima

The logotype

This page contains camera-ready reproduction artwork for the Prima logotype. This logotype can be reproduced for larger-scale work pertaining to the individuals' rights on the privacy of their data.

This logotype is meant to be seen across the nation to educate the public on their unspoken rights that they have to protect themselves, and all of their loved ones around them from all of the dangers of our personal information being used against them. The logotype is not meant to instill fear within the American public, but rather just be an informational guide to help keep themselves safe and know that we are one united nation that should not be scared of their neighbors, their friends, and any person online — however in order to do so they must take precautions to protect themselves across all platforms.

Typeface

To remain informative and purposeful, the Prima brand uses Helvetica Medium across all mediums for ultimate legibility. The point of this movement is spread the Prima message loud and clear for the entire nation to understand how exactly important data privacy should be to them, even if they don't feel any sense of danger. This typeface is used as a neutrality standing to the public. We are not here to act amongst a higher power, and we are not here spreading this message of fear. It is always Prima's goal to maintain authenticity and reliability for all to understand what this movement really can mean if we can get every single American — young and old, to treat their privacy accordingly and responsibly.

Combination mark

Paired with the reliable logotype, this combination mark reveals the type sitting inside the enclosure of the Prima square. This square finished off with a singular corner radius is meant to symbolize a starting point filled with trust and ease. We wish to remind every American that we are indeed safe, but there must be a starting point into protecting our privacy, allowing there to be an open two-way conversation of knowing what we can protect and what we can stay cautious of. This combination mark should only be used in appropriate environment leaving one inch around each side of the perimeter of the Prima square to separate the safety of the Prima brand away from intrusion of our data.

Bounding box for appropriate and authentic usage of the Prima logo.

Privacy means protection.

Step 1

Back Up Your Data

Why back up

We are here to empower the people and promote action. Prima is not here to sell you any product, we are not here to sell you an idea. Instead, this agency is here to inform the American public about the rights that are indeed put in place to protect them that may be unknown to them, but also inform them of steps they can take.

In order to start your journey into protecting yourself, you should always make sure that you are aware of where you are keeping your information, and what exact information you are using wherever you go. It is easy to lose track of what information you use on a daily basis because everywhere we go, everything we do, everything we look up, we are leaving data and personal information in our tracks. To get around this, it is important to take note elsewhere of what information and data you use.

Email addresses, names, card information, birthdays, hometowns, passwords are just a few amount of the things that we give away on a daily basis to companies, people, both of which can be people we trust with our lives, or not even know at all.

How to back up

In order to back up your data, this would require you to make sure you putting any information you want to keep safe in multiple locations. It is important to use external sources keep your data secure. Whether this means storing a backup set of information on a different application, writing it down, a different site, of external device such as a hard drive or flash drive, this will allow you to make sure that your data will always be in a different location than where its original source is from.

No matter what you do it is important to protect this information, and this includes whatever back up pieces you are making for it.

When using tools such as external devices such as hard drives or flash drives, it is vital to encrypt them. This means taking measures to put locks on it to prevent unauthorized access from unwanted users. With physical documentation, it is a good idea to put information in a lockable cupboard to ensure safety.

What is it for

It may seem a bit dramatic, but any information you would consider to be important to you is the exact information that you should be making sure stays safe. This could be information about yourself and your life, or even the other people in your life as well. It is very important to take matter into your own hands.

It can seem scary, but this does not mean you cannot put any information out for anyone to see — that is not our goal in creating this agency whatsoever. Instead, the focus is to make sure that every American is conscious about the information they are putting out, knowing exactly what they are doing and why they are giving the information they are giving at any said moment.

Span the horizon

At the end of the day, our information is everywhere, and there is no way around it. We have to give our information everyday. For this reason, you must know that your protection should be universal. You can't just be backing up data or information online, or just information you give in person, but you must focus on both.

It is a daunting task to maintain your constant focus on every single thing you do — but you can do whatever you feel is the most safe to you. It is hard to cover yourself on all bases, but you should know where you feel like you're giving information you don't believe is necessary to be revealing or information you are sensitive about.

No matter how large or small scale the information may seem, it is always okay to keep precautions, even on places you do feel safe on. Breaches of personal information can be scary, and can happen even within things you trust, so the only thing you can do is prepare and make sure you have plans set up in case of something happening to your information.

What is the concern

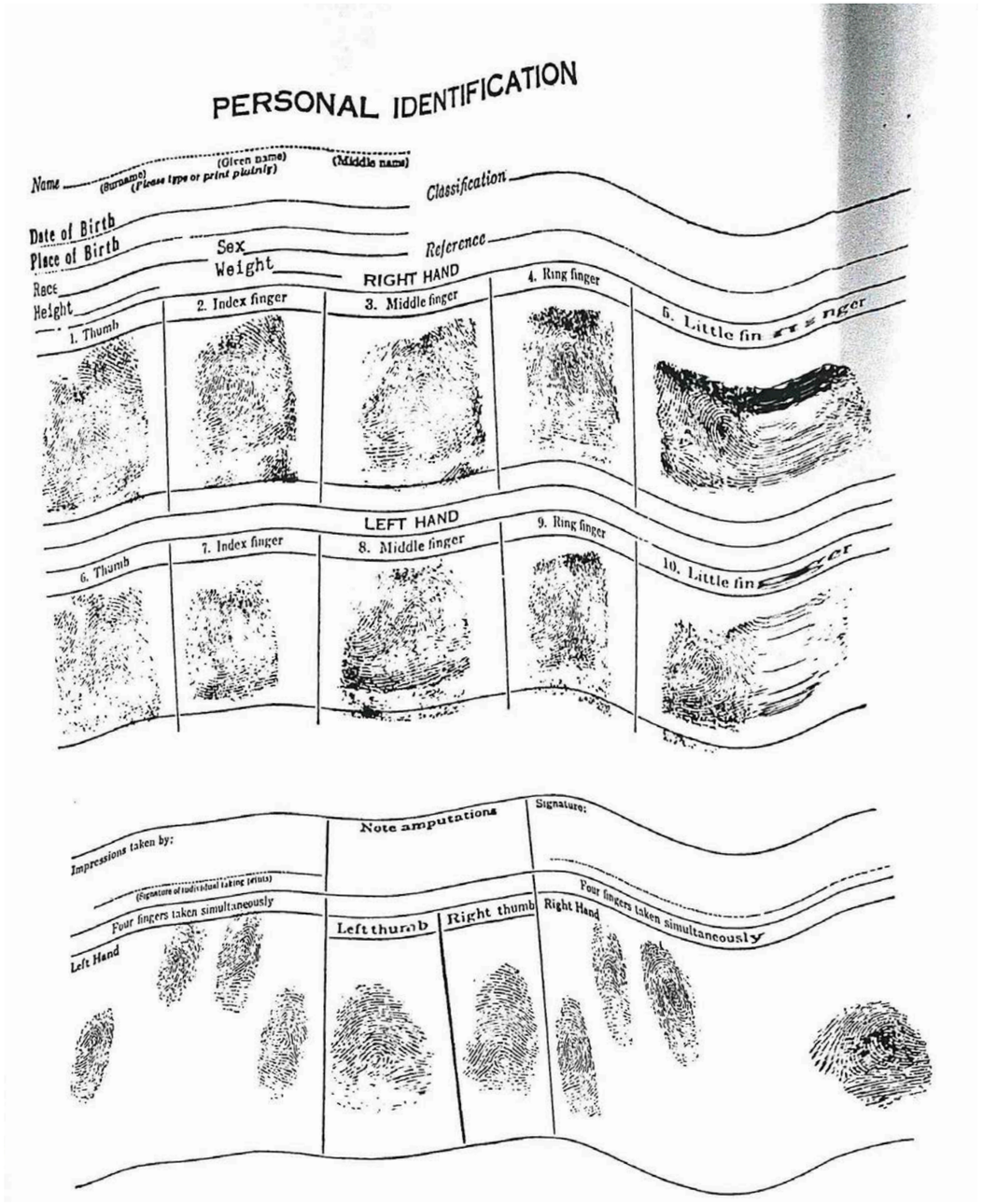
Your data and information is very specific to you. Personal is defined as: “of, affecting, or belonging to a particular person rather than to anyone else” in the Merriam-Webster Dictionary. Maintaining your identity isn’t an everyday concern the typical American has running through their head, but this information can be compromised with ease, sometimes even without us knowing.

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers’ trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.

Some businesses may have the expertise in-house to implement an appropriate plan. Others may find it helpful to hire a contractor.

Your personal information at times lies in other people’s hands, and it is very easy for someone to easily steal and make copies of your information, and use it as their own. Traditional practices of keeping safety are going out of date, as thieves become smarter and have easier access to any and all information, you can easily lose all of what exactly makes you, *you*.



Protection

Despite being the biggest online market in the world, it's only now that the USA has come up with adopting more laws to ensure the rights of users to digital privacy. As of now, digital privacy is guaranteed on a federal level by four acts: The US Privacy Act of 1974 (concerns the data held by government agencies), The Health Insurance Portability And Accountability Act (HIPAA) of 1996 (refers to the data processed in healthcare sectors), The Gramm-Leach-Bliley Act (GLBA) of 1999 (financial nonpublic personal information), The Children's Online Privacy Protection Act (COPPA) of 2000 (protects information of kids under 12).

State-wise, there are only a few (California, New York, Maryland, Massachusetts, North Dakota, Hawaii) that have pursued creating a comprehensive law to cover digital privacy issues regardless of the sphere. One of the closest to an ideal one is the California Consumer Privacy Act of 2018. Under this law, consumers get the right to know exactly how their data is used by covered businesses by sending a data subject access request (DSAR).

Also, companies can't sell customer data, and customers can ask to get their data deleted (except for those required for storing by law). In 2023, this act will be accompanied by the California Privacy Rights Act. This will include broader definitions of 'sensitive data,' increase the threshold for handling records and add the right to correct the data.

Organizations such as the GDPR (logo pictured left) help with your online protection, it doesn't guarantee safety before disaster strikes as following in the next section. While these protections are still slowly coming into place, you must make sure you are taking care of yourself in the mean-time as more laws get approved and put in place.

Living is easier with data protection.

Don’t lose what makes you, *you*.

Step 2

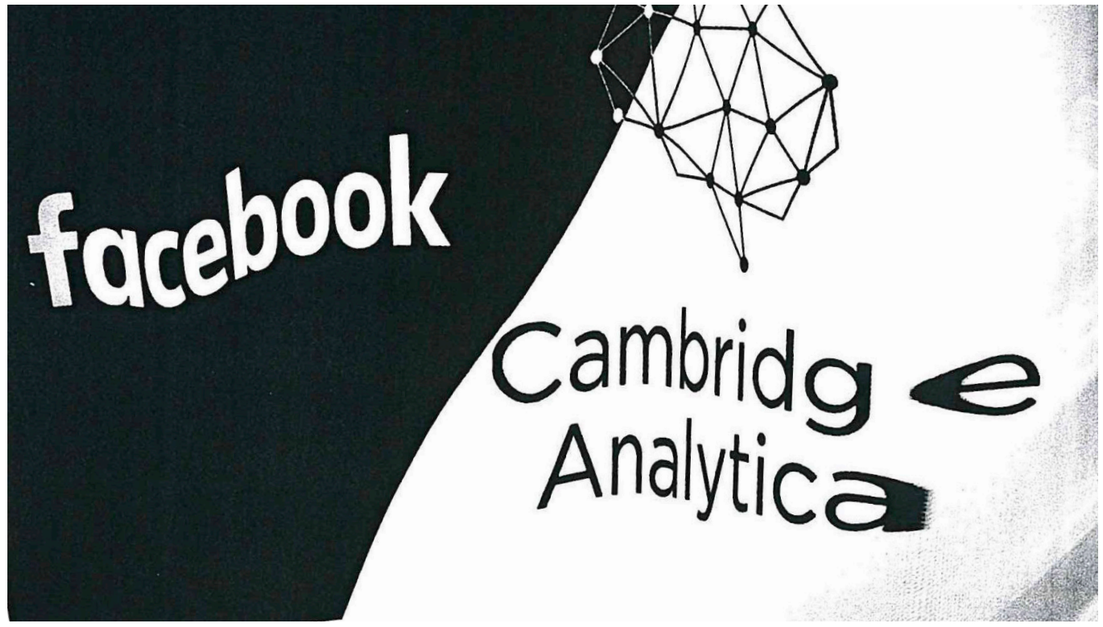
Secure Your Accounts

In the public eye

The data harvested from our personal devices, along with our trail of electronic transactions and data from other sources, now provides the foundation for some of the world's largest companies. Personal data also the wellspring for millions of small businesses and countless startups, which turn it into customer insights, market predictions, and personalized digital services. For the past two decades, the commercial use of personal data has grown in wild-west fashion. But now, because of consumer mistrust, government action, and competition for customers, those days are quickly coming to an end.

Many people have mistrust in the government and what all exactly they do with our information and data. There have been many scandals recently that have come to light thanks to new regulations being put in place around the world.

The new digital age now requires Americans to take extra precautions with their digital footprint and what information they give to the wrong people. It is becoming easier and easier to replicate identities and easily swindle ways into your personal information which draws greater attention to securing your accounts and information. Without being secure in the information you're putting out anywhere, you're losing the potential of maintaining safety and possibly falling victim to having your information hacked. These breaches can take place anywhere and at any time we may even least expect it.



Its impact on privacy

In March of 2018, the Guardian and New York Times simultaneously published stories on how the personal data of over 50 million Facebook users ended up in the hands of Cambridge Analytica, a company which sought to increase support for the 2016 Trump presidential campaign.

The company's work had been reported before, for example, for US Senator Ted Cruz using Facebook data had previously been reported in 2015, but the March revelations propelled the company to worldwide attention, perhaps due to the scale and potential links with the 2016 Brexit referendum and the 2016 US presidential election.

Cambridge Analytica was a consulting and data analytics company that was funded by right-wing American billionaire Robert Mercer and headed by Breitbart-founder Steve Bannon before he left to serve as chief executive for the 2016 Trump campaign. Reporting covered how Cambridge Analytica used data to profile and target individual voters with the aim of predicting and influencing their voting decisions. Reporting further revealed that Cambridge Analytica also supported the Brexit campaign in the UK.

According to the Guardian and the New York Times, by late 2015, Facebook was aware that Cambridge Analytica had exploited its users' data, but Facebook failed to inform people who were affected and engaged in limited and ineffective efforts to recover their data. Facebook later admitted that the number of people affected was much higher than what the Guardian and New York Times had initially reported: it had actually shared the data of 87 million users.

The scandal and its impact are thanks to the persistence and dedication of a number of individuals, including investigative journalists such as Carol Cadwalldar, researchers, the whistleblower Christopher Wylie (a former employee of Cambridge Analytica), Shahmir Sanni (a volunteer with the Vote Leave Campaign in the UK Brexit Referendum), and Professor David Carrol, a New York-based professor, who has engaged in a lengthy battle to obtain his data from Cambridge Analytica.

The story that broke in March 2018 was not the beginning or the end. Over a year since, more information and questions have emerged.

Furthermore, Cambridge Analytica's role was by no means limited to the UK and US. It was involved in elections around the world. Privacy International had previously looked at the role of Cambridge Analytica in the Kenyan elections and as the revelations unfolded we provided an update in response to the focus, and our Kenyan partner CIPIT further examined the role of the company.

Among other developments in the United States, the Department of Justice, Federal Bureau of Investigation, the Securities and Exchange Commission, and the Federal Trade Commission have been examining Facebook's data sharing and protection practices. This includes a new investigation into the Cambridge Analytica revelations.

On April 24, 2019 it was reported that Facebook expected to be fined up to $5 billion by the Federal Trade Commission for privacy violations, which would be a record fine imposed by the FTC against a technology company. Facebook disclosed this amount in its quarterly financial results, saying that it expected a one-time charge of $3 billion to $5 billion. Furthermore, federal prosecutors in California are still actively investigating the Facebook-Cambridge Analytica scandal to this day.

Given the low overall levels of trust, it is not surprising that consumers often want to restrict the types of data that they share with businesses. Consumers have greater control over their personal information as a result of the many privacy tools now available, including web browsers with built-in cookie blockers, ad-blocking software (used on more than 600 million devices around the world), and incognito browsers (used by more than 40 percent of internet users globally). However, if a product or service offering—for example, healthcare or money management—is critically important to consumers, many are willing to set aside their privacy concerns.

Consumers are not willing to share data for transactions they view as less important. They may even "vote with their feet" and walk away from doing business with companies whose data-privacy practices they don't trust, don't agree with, or don't understand. In addition, while overall knowledge of consumer privacy is on the rise, many consumers still don't know how to protect themselves: for example, only 14 percent of internet users encrypt their online communications, and only a third change their passwords regularly (data from McKinsey).

Look around you

People have been trusting big firms such as Google and Facebook with their data for years. They have offered their location data to Google and information about their preferences to Facebook so they can be targeted with so-called 'personalized' advertising. But these companies are proving that they can not be trusted with people's data.

So, of the other massive companies that collect user data, who can be trusted? Amazon prides itself on security: users will potentially allow its delivery people access to the inside of their homes when they aren't in. Its Amazon Echo speaker is selling millions – although in May, the Google Home sold more, according to figures from analyst Canalys.

Apple also has a good reputation for security. So much so, that in April, the firm ranked top in a privacy survey. The survey, a collaboration by SurveyMonkey and Recode, asked "Which of the following companies do you trust the least with your personal information?"

Just 2% of respondents answered Apple and Amazon, while Facebook and Google were the least trusted.

Apple has historically been vocal about protecting user information, while also working with law enforcement when they have subpoenas and other legal requests for data.

Both Apple and Amazon have been implicated in the recent China 'spy chip' scandal, but they deny the claims.

Security breaches will continue to take place, but trust in technology companies is falling. If the likes of Apple, Google, Facebook and Amazon want people to continue to use their services, they need to demonstrate how they protect data. If an event does happen, their response is what matters. With GDPR regulation stipulating huge fines for firms that fail to safeguard user data, perhaps things will improve. For now, it's up to users to decide which technology companies they trust.

The bottom line is that regardless of your level of trust, it is important to make sure if you are using applications that do require you to share personal information of your own, that you are willingly doing it and know how this application is going to use all of the information they are getting from you. In this day and age, it is hard not to share so much information regarding your day-to-day life, celebrations of career success, love, or any other type of accomplishment — we are human. We are meant to share, but we need to know the risks of sharing. While you can very easily enjoy sharing special moments in your life, staying protected and securing your social media accounts, banking information, and other type of information you might want safeguarded is ultimately the best choice you can make for yourself.

The big community

We have to realize we are sharing our information with the rest of the world. You are not alone, as everyone else is sharing similar levels of information as most others are, but it is important to note the risks of it. Most people just simply want to keep their information safe, but there are a few people and organizations that do have malicious intent with taking others' information. This is not meant to scare you as more regulations protecting your safety are coming in place, but rather to keep you informed and aware of the potentials of what could be in happening in your own life, or even the people around you. We are all one big community, and we need to make sure we are protecting one another.

Privacy is a
matter you
can’t avoid.

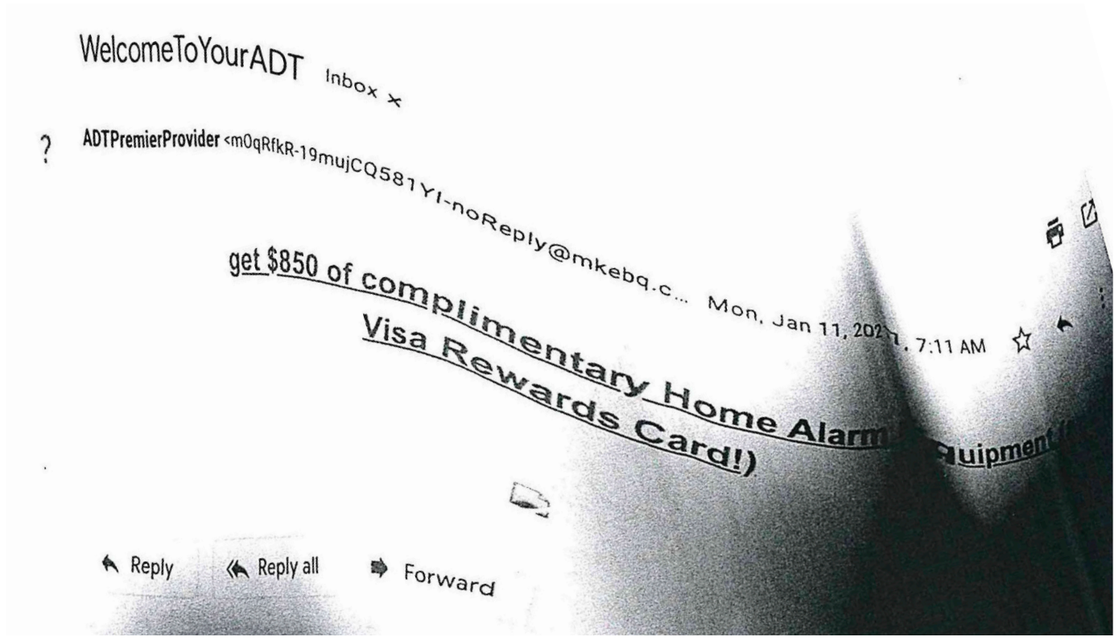
Step 3

Protect Web Browsing

Targeting

Companies and websites track everything you do online. Every ad, social network button, and website collects information about your location, browsing habits, and more. The data collected reveals more about you than you might expect. You might think yourself clever for never tweeting your medical problems or sharing all your religious beliefs on Facebook, for instance, but chances are good that the websites you visit regularly provide all the data advertisers need to pinpoint the type of person you are. This is part of how targeted ads remain one of the Internet's most unsettling innovations.

A lot of scams and fraud take effect on targets that very easily make themselves vulnerable. In order to do this some scammers will go out of their way to target certain demographics in order to allow their plan to go according to plan. This typically may mean that users of a much younger and much older demographic may be more susceptible to attacks over the phone, over mail, and/or over social media platforms. This goes back to all of the websites you visit online. These attackers are aware of what scams they can use to specifically target you for your needs. It's important to be very weary of what emails you open, and to take extra care in deciphering what is a legitimate email, phone call, message that is in your possession.



Attackers can create emails posing as someone else with attached links that likely contains malware which will then damage the user's computer, or will prompt them to enter sensitive information that will hurt the user.

Phishing

Phishing is a popular form of cybercrime because of how effective it is. Cybercriminals have been successful using emails, text messages, direct messages on social media or in video games, to get people to respond with their personal information. The best defense is awareness and knowing what to look for. Some tactics of phishing include an urgent call to action or threats, first time senders, bad grammar and/or spelling, mismatched email domains, generic greetings, and suspicious or unexpected links or attachments. These are just some of many things to look for.

Cyber criminals can also tempt you to visit fake websites with other methods, such as text messages or phone calls. Sophisticated cyber criminals set up call centers to automatically dial or text numbers for potential targets. These messages will often include prompts to get you to enter a PIN number or some other type of personal information.

Never click any links or attachments in suspicious emails. If you receive a suspicious message from an organization and worry the message could be legitimate, go to your web browser and open a new tab. Then go to the organization's website from your own saved favorite, or via a web search. Or call the organization using a phone number listed on the back of a membership card, printed on a bill or statement, or that you find on the organization's official website. If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it. Report the messages and then delete them.

Messages requesting immediate action typically are those of scams deliberately trying to get you to give up some personal information for a fake company.

Managing cookies

A cookie is a small text file processed and stored by a web browser to remember information about a user. When a user visits a website, a cookie is downloaded into their web browser and stored as a plain text file. When the user visits the same website again, the website reads the cookie and knows it's the same user.

Over the years, computer cookies have earned an unsavory reputation, but they are not inherently bad. They are simply a mechanism to how the world wide web works. However, since some companies utilize cookies to capture data to create detailed user profiles to sell to other third-party companies for marketing and advertising purposes, some users have grown a little bit wary of the intentions of cookies.

Bottom line

At the end of the day, our information is everywhere, and there is no way around it. We have to give our information everyday. For this reason, you must know that your protection should be universal. You can't just be backing up data or information online, or just information you give in person, but you must focus on both.

It is a daunting task to maintain your constant focus on every single thing you do — but you can do whatever you feel is the most safe to you. It is hard to cover yourself on all bases, but you should know where you feel like you're giving information you don't believe is necessary to be revealing or information you are sensitive about.

No matter how large or small scale the information may seem, it is always okay to keep precautions, even on places you do feel safe on. Breaches of personal information can be scary, and can happen even within things you trust, so the only thing you can do is prepare and make sure you have plans set up in case of something happening to your information.

Your privacy is in your hands.

Step 4

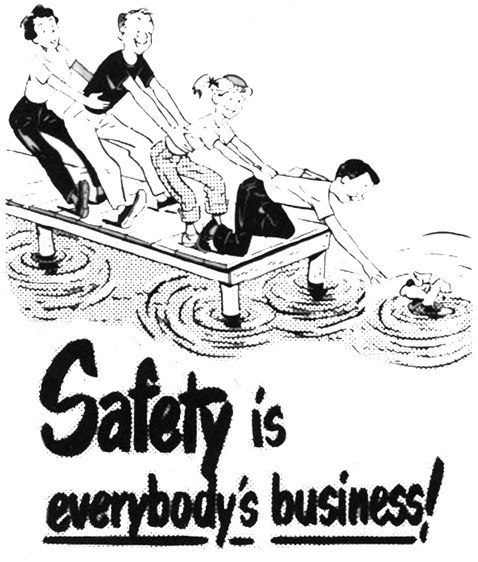
Protect Each Other

Who is impacted

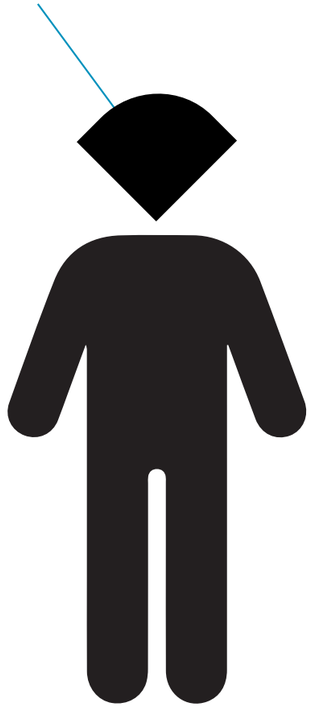
Data breaches hurt both individuals and organizations by compromising sensitive information. For the individual who is a victim of stolen data, this can often lead to headaches: changing passwords frequently, enacting credit freezes or identity monitoring, and so on. Depending on their due diligence efforts to protect the data in the first place, the organization which was compromised may be on the hook for the cost of monitoring services for victims after a breach. They will also be responsible for notifying victims about what information was stolen during the breach.

Altogether, it can be an expensive lesson in data security – IBM reports that the average cost of a data breach is almost $4 million USD. And, there's the non-monetary cost of a tarnished reputation.

There are about 3,800 openly disclosed breaches within a span of a year, many of which can happen to larger organizations. As seen within the Cambridge Analytica scandal, millions of users were impacted just based off of one scandal. These breaches have larger impacts than just yourself and can put your work and.or loved ones in danger.



You, impacted by a breach of your personal information.



Everyone else who could be impacted by a breach of your personal data.

Scope of precaution

Viruses might not seem as common as they were a decade ago, but they still exist. Malicious software on your computer can wreak all kinds of havoc, from annoying pop-ups to covert bitcoin mining to scanning for personal information. If you're at risk for clicking perilous links, or if you share a computer with multiple people in a household, it's worthwhile to set up antivirus software.

Taking the step to keep your browsing safe for everyone around you is important. Any type of data, documents, or just information you keep up for too long or allow to get in the wrong hands not only affects you by others around you as well. Even starting at making sure you're using things such as a secure WiFi network could save you from a breach. Being aware of your surroundings is the most important initial step into putting up enough safeguards.

Vulnerability

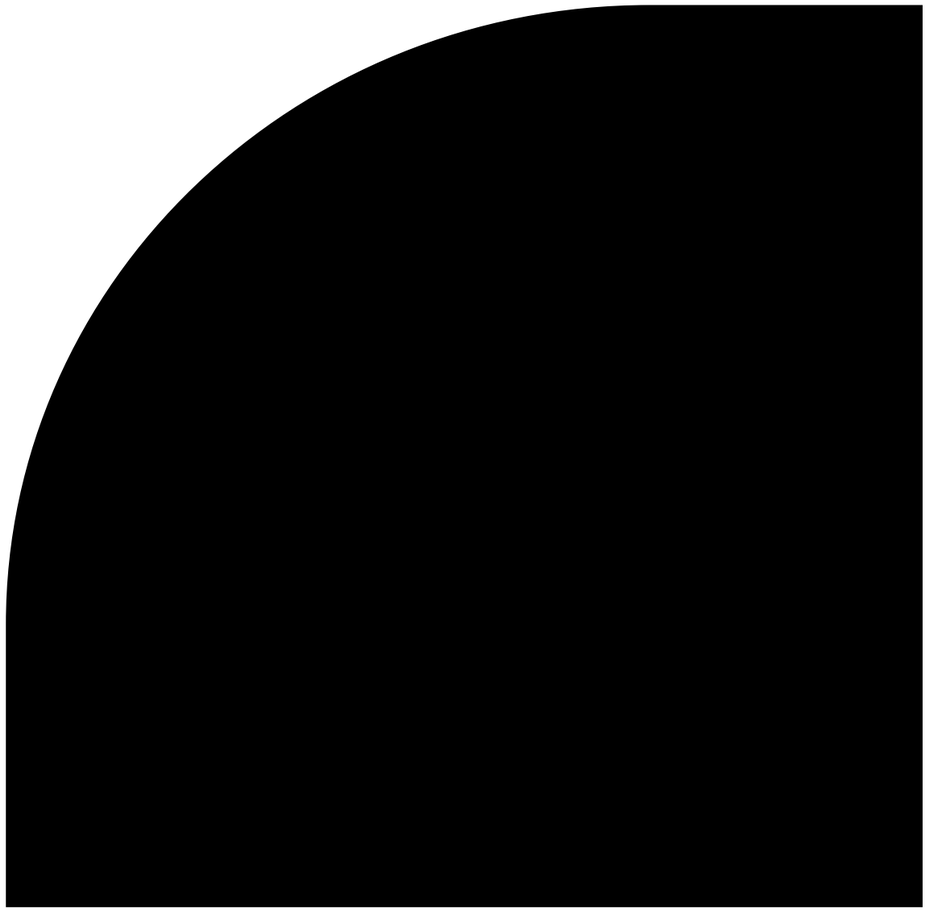
All of this information may be a lot to take in all at once, and it may seem overwhleming to the point of instilling fear, but that is far from the goal. There are so many precautions out there to take in order to protect your privacy — the issue is the lack of knowledge individuals are given regarding their safety and how they could be impacted.

The United States are in the process of attempting to put laws in place protecting our data privacy rights, but they are slow, and very limited state-by-state at the moment. In the meantime, this manual provides steps that can be taken, as well as topics to look further into regarding many different topics on our personal data privacy that should be looked into for the sake of your safety, as well as all of those around you.

Attackers are always going to be out there regardless, and they are always willing to prey on those who are the most vulnerable in order to make an easy target. This is why it is your responsibility to make sure you are doing everything you can in order to be prepared for the potentials of what could happen, and more conscious about the messages we open, as well as the information we are giving out to people sometimes could even pose as someone you personally know, or someone who claims they have more expert knowledge on the matter, which could be a complete and udder stranger that is from all the way across the globe.

This man is content while sleeping with arms closed off covering over the information in his hands, that could very easily be taken if he were to doze off and not pay attention at all.

Even though he looks content, his crossed feet show signs of fear, which he wouldn't have if he knew the proper procedure to take in order to protect his own privacy.



Foreword

As a foreword, here at Prima, we wish to finally extend a hand out, offering help to those who feel unprotected and fearful of their personal information being taken from them. The world around you is a very dangerous place and while there are slowly but surely measures being put in place to help your personal security, there are actions you can take to even further your chances of keeping your identity and data safe.

Whether you want to take precaution on your social media accounts, your banking information, confidential work data, or just sensitive personal information — now is the time to act. The longer you take to wait on protecting your information, the more data you will build up, which could leave you with more information to lose. This Prima Manual is created with the intent of shedding light on this manner that is rather disregarded. For further help and guidance in protecting your personal information, please visit our website at: **primanual.com**, for more information.

Seriously.

Take control
of your data.

prima