Consumer Guide to Protecting Privacy Online

As part of Attorney General Gansler's continuing education efforts on Internet privacy, the Internet Privacy Unit has created a web-based **Consumer Guide to Protecting Privacy Online**. This Guide helps explain what "personally identifiable information" is, how it is collected and treated online, and how you can protect it, offering links to the state and federal laws that set out your online privacy rights. It also offers tips for being a privacy-savvy user of Internet websites and services and Internet-connected mobile devices. We hope you find it to be a valuable resource. The guide covers:

- What Is Personally Identifiable Information, and Why Is It Important?
- Where Do I Go To Learn How Companies Treat My Information?
- What Can I Do To Protect My Information Online?
- Cookies and Online Tracking
- Using Social Networks & Photo-Sharing Services
- Mobile Devices & Privacy
- Additional Privacy Considerations
- Online Privacy Rights under Maryland and Federal Law

This guide was created in collaboration with the Future of Privacy Forum, a non-profit think tank that seeks to advance responsible data practices, with an advisory board comprised of leading figures from industry, academia, law and advocacy groups.

What Is Personally Identifiable Information, and Why Is It Important?

As you conduct more of your daily life online, you often are asked to disclose Personally Identifiable Information (PII) - information that uniquely identifies you. PII includes information like your name, address, phone number, birth date, Social Security number, credit card and bank account numbers. Other types of information, such as your age, your religious faith, marital status, and shopping history can be combined together by marketers and other third parties to develop profiles about you. Websites you visit and apps you use may also collect information about you in the background, without you affirmatively inputting it, through the use of "persistent identifiers." These are things like Internet "cookies" and mobile phone hardware identifiers (like device IDs), and although they may not identify you by name, they can be used to track your web surfing and to tailor which ads you are shown. Cookies can also store PII about you if you provide it. (See the section entitled "Cookies and Online Tracking" for more information.)

Sharing your PII with people and companies you trust can provide you with many benefits and services. Companies often need such information so that they can fulfill your requests or offer you their services. For example, you need to give a name and email address to sign up for most social networking services. And, if you order merchandise from an Internet merchant, you need to tell the company your address so it can deliver the purchase to your home.

On the other hand, if you are not careful about what PII you provide, and to which companies, it may be used in unexpected or undesirable ways. Your information could be shared without permission with other companies, resulting in unwanted marketing or intrusive advertising. Also, by sharing your PII - especially with individuals or companies that you do not know and trust - your data could be lost, stolen, or fall into the hands of fraudsters or identity thieves. This is why it's important to think before you share your PII.

Where Do I Go To Learn How Companies Treat My Information?

Many companies have privacy policies that tell you how they collect, use, and share your information. By reading a company's privacy policy *before* you use that company's product or service, you can learn what information it collects and how it will use and share it before you decide whether to give out your personal information. The existence of a privacy policy does not necessarily mean that your privacy is protected. A company's privacy policy is often where a company tells you how they will use and share your data, if you have any choices about how your data is used or shared, and how to exercise those choices. You can usually find a link to the "privacy policy" or "privacy notice" near the top or bottom of a company's home page.

In addition to privacy policies, some companies may display familiar seals or "trust marks." You might recognize some of these examples:

Seals like these indicate that the company has committed to follow a set of agreed upon privacy rules. They also provide another resource you can contact if a business has violated a privacy commitment. However, if you are concerned about the treatment of your PII, you should read the privacy policy, rather than relying on seals or "trust marks."

What Can I Do To Protect My Information Online?

There are a number of steps that you can take to limit and protect the information that you share online. These include:

Use Settings and Controls. Know your options. Take the time to understand the controls or "settings" for the products and services you use. They control what information you share with others and may include important choices. For example, often the privacy settings of a web browser will allow you to limit the placement of some types of tracking cookies.

Share PII with Caution. Remember, if you give your information to people or companies, they may share it with others - including advertisers, family members, employers, or other third parties. Be wary of companies that may not protect the information you share, or may use your private information in unexpected ways. And remember: "free" on the Internet often means that you must give up your PII in exchange for using the product or service.

Use Strong Passwords. Strong and secure passwords are an important tool to protect your privacy and the security of your information online. Take password security seriously and create challenging passwords that will be difficult for others to guess. Some tips for building a strong password include:

- Don't use your name or birthdate - be unpredictable
- Make your password at least 10 to 12 characters long, and use a mix of letters, numbers, and special characters (like %, $, #, or @)
- Don't use the same password for multiple accounts
- Keep your passwords in a secure place, and don't share them with anyone - especially over the phone, in texts, or by email

Only Give Your PII to Secure Sites. If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for *https* at the beginning of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session is not encrypted, the entire account could be vulnerable. When shopping or banking online, look for *https* on every page of the site you're on, not just where you sign in.

Consider "Extra" Security Steps. Increasingly, online services such as email, social networking sites, and cloud storage providers, are offering more advanced tools to protect your passwords and the security of your account. "Two-step authentication," for example, requires a code sent in real time to your mobile phone in addition to your password to let you log in to an account or service. This makes it harder for anyone other than you to access the information in your online account. Consider using these extra security measures where they are offered.

Keep Your Web Browser and Antivirus Software Up to Date. Out-of-date web browsers and antivirus software can leave your computer vulnerable to attack by malware, which could capture sensitive data like your log-in information, passwords, or financial information. Antivirus software will prompt you to update to the latest version, and most browsers will either do the same or update automatically.

If You Suspect You Are a Victim of Identity Theft, Report It. Identity theft occurs when someone uses your PII to pretend they are you. Identity theft can allow someone to run up debts on credit cards in your name, open new credit accounts in your name, take your tax refund, or make it harder for you to find and keep employment. For more information about identity theft and how to prevent and report it, go to http://www.oag.state.md.us/idtheft/ or http://www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also contact the Attorney General's Identity Theft Unit by calling (410) 576-6491 or by sending an e-mail to idtheft@oag.state.md.us.

Cookies and Online Tracking

In addition to collecting PII, companies also may collect other information about your computer or device behind the scenes. For example, as you surf the Internet using a web browser, sites can place "cookies" on your computer. A cookie is a small file that allows a website to store data about your browsing activities, including identifying the pages and content you've looked at, when you visited, what you searched for, and whether you clicked on an ad. Cookies can be used to help websites remember things like which items you place in an online shopping cart, or your log-in information or preferences for future visits. Cookies can also be used to create a profile of your online activities so that companies may deliver ads tailored to your interests. While some people may like having ads tailored to their interests, others may find such targeted advertising undesirable or intrusive.

There are a number of steps that you can take to control the cookies placed on your computer, or to opt out of targeted advertising:

- **Use Your Web Browser Tools and Controls.** Many browsers have different ways that you can delete cookies or limit the kinds of cookies that can be placed on your browser. For example, look under "Tools" or "Safety" in your browser for settings like "Options" or "Privacy," and review what controls and deletion options are available. Some browsers also permit you to install plug-ins or add-on tools that can block, delete, or control cookies.

  Many browsers also offer "private browsing" tools so that your online browsing can be kept hidden from other people who use the same computer. When these features are turned on, your browser typically won't keep cookies, browsing history, search records, or the files you download. These tools are not the same across all browsers, so it is important that you check to see what kind of data your browser stores.

- **Do Not Track Features.** Browsers provide users with "Do Not Track" settings, but how websites respond to this signal is not yet standardized. For more information about the developing Do Not Track standard and how companies will treat your choices, visit www.allaboutdnt.org.

- **Consider Opt-Out Cookies.** A number of advertising networks and other companies that set third-party cookies on browsers offer consumers the ability to opt out of receiving these cookies and the targeted ads they enable. For example, programs from the Digital Advertising Alliance and the Network Advertising Initiative offer tools for opting out of targeted advertising - typically using cookies - for their members. These ad networks will still collect data and deliver the ads you see, but those ads won't be selected based on a profile on your web surfing. Just remember that if you delete all your cookies, you will delete your opt-out cookies as well, and will have to go through the procedure again to restore your opt-out cookies.

Note that cookies are just one tool used by third parties to track you online. Other tools include web beacons (also known as "web bugs"), pixel tags, and device fingerprinting. These tracking tools may provide you benefits, like more relevant ads and more convenient online experiences, but remember that, unless you have taken affirmative steps to reduce or prevent tracking, your browsing will likely be tracked in some way. (For more information on tracking, see the section entitled "Mobile Devices & Privacy")

Using Social Networks & Photo-Sharing Services

Social networks and photo sharing services are great ways to connect and share with friends, family, or colleagues. However, it is important you understand what information you're sharing and with whom. Otherwise, the photo you wanted to share with only your closest friends may also be viewed by potential employers, relatives, or other unintended audiences.

Three Guiding Principles for Using Social Networks & Photo-Sharing Services:

1. **Think First.** Information you share on social networks can sometimes become public without your permission, and your friends on the network may pass along information that you did not want them to share. Always be cautious about sharing anything about yourself that you would not want widely known (such as a sensitive medical condition). Assume everything that you post online is *permanent*, even if the post has an expiration feature. When you upload photos and post comments online, be aware of your audience. For example, your settings on a social network may allow the photos and posts you share with friends to also be viewed by your friends' friends, whom you've never met. Take advantage of social network features that allow you to share information only with the audience you choose. Also, consider the privacy interests of your friends before sharing their information with others. They may appreciate you asking before you post that picture of them! *In general, think carefully before sharing something that might be made public*.

2. **Know Your Choices.** Social networks often come with controls or settings you can use to determine how to share your information with other people. Some social networks let you decide whether to share information just with friends or with a broader group, including the general public. Some information you share with social networks may *always* be public, and not subject to controls. You may share other information publicly based on the *default* policies, but you may be able to change your settings to limit this sharing. Sometimes you may also have the choice to override default settings and prevent certain information from being seen by all but a select few. Social networks vary widely in what information is made public and subject to controls. *You should always read and review the privacy options your social networks offer so that you know your choices.*

3. **Choose & Test Your Settings.** Once you've reviewed the choices you have, choose your settings. Don't accept the default settings unless they represent the degree of privacy and sharing that you want. Where possible, check what information other people can see about you online. Some social networks allow you to preview what information others can see on your profile with a special tool, but you can also test this by logging out of the service and checking to see what is visible to the public. Your privacy settings may also interact with those of your network friends. For example, when you label or "tag" a friend in a posted picture, this information may become available - perhaps by *default* - to all of your network friends and to all of *their* network friends. That's why it's just as important to test your settings as it is to choose them.

Other Issues to Consider About Social Networks & Photo-Sharing Services:

Employer Access to Your Social Network Information. Maryland was the first state in the country to prohibit employers from asking for your username or password on your private social network. *It is against the law in Maryland for an employer to take or threaten to take any sort of adverse action against you based on your refusal to share this information.* If you keep information on your social network account private and access the account only from your home computer, personal cell phone, or other private, personal devices, your employer has no right to access the information.

In general, however, when you use *employer-provided* computers, telephones, or cell phones, employers that inform employees about workplace monitoring can track employee activities. This means you should think carefully before visiting your personal email account or social networking service, or conducting personal banking or other affairs, using your workplace computer.

Apps and Social Networking. Social networks often support applications, or "apps" - programs that may make your network more user-friendly or enjoyable. These might include games you can play with your friends, the ability to access and sync information from multiple devices, or permission to log into various other websites using the same username and password as on your social network.

Apps can also make it easier to tie your other online activities to your social network. Using apps generally gives app developers access to some basic account information about you, and they can collect additional information in order to personalize your experience or show you marketing. You should always examine your apps' privacy notices. Many apps will have different privacy policies from your social network, and will provide different security or protection for your personal data.

Your Friends. Apps may share your information with your friends or even all the members of your social network. Apps may also collect information about you and your friends or connections. For some apps, you may choose settings that let you use the app while limiting the information it may collect or share. However, not all apps have such settings, which is why it is important to review app privacy policies and settings before you download and use them.

You should also be aware that your friends can give their apps access to your information as well, sometimes without your knowledge or approval. If you do not want an app to access your information, you may need to disable it, which some social networks offer as an option. For all of these reasons, it's also important that you *truly know* the friends with whom you are connecting online.

Reporting Abuse. Social networks have different policies for addressing abusive behavior, but most services allow users to report abusive behaviors, threats, and privacy violations. Read the Terms of Service to learn more about how to report problems with online bullying or abuse.

Mobile Devices & Privacy

Tablets and smart phones - like the iPhone, Android phones, and Blackberry phones - are incredibly popular. They offer great services and tools, such as the ability to download and use apps, search the Internet for driving directions, and make purchases on the go. They also come with features that affect your privacy in ways desktop computers and landline phones don't.

Location Information. Mobile devices like smart phones and tablets include technology that allows companies to collect and sometimes share your location information, often in real time. You may want to share this information with friends so they know where to meet you for dinner, or you may want an app to know your location so that you can find a nearby restaurant or get directions. However, you may not want to share location information with companies that don't need to know your location, for example the developer of a game app. Also, by uploading and sharing photos that reveal your location, you may give friends and strangers alike the ability to know where you are, where you have been, or where you habitually go. Location information not only can tell friends and trusted companies your location; it can also allow strangers to know when you're away from home, or allow others to figure out where you're spending your time when you do not want them to know. Retailers may track the WiFi or Bluetooth signals from your cellphone to create reports that they use to monitor wait times online or to analyze the location of shoppers. You can turn off WiFi or Bluetooth when you don't need it to avoid this tracking and can visit www.smartstoreprivacy.com for opt-out options offered by location companies.

Use Your Settings. Although smart phones differ in how they handle location information, most allow you to adjust or "toggle" location data sharing. These controls can be found in your devices' settings. Some settings allow you to turn off location services entirely, while others allow you to control individual apps' access to location information. When you do not explicitly need your location information for an app or service, consider toggling off location services to protect your privacy.

Password-Protect Your Device. Consider adding a password to protect your smart phone or tablet. That way, if it gets lost or stolen, it will be harder for others to access the information about you on it. Many smart phones also have features that allow you to remotely delete your private information in the event your phone is lost or stolen.

Additional Privacy Considerations

Children and Teens. Today, children have access to computers, smart phones, tablets, video services, and other devices - and each of them raises privacy concerns.

If your children are under the age of 13, the federal law known as the Children's Online Privacy Protection Act (COPPA), applies to the collection of their personal information. When websites are directed towards children under age 13, they may only collect your child's personal information where there is clear, verifiable evidence that you consented to provide the information. They must also honor your choices about how the child's data will be used. Both the Attorney General and the Federal Trade Commission have the authority to take action against a company that violates COPPA.

Do not allow your children to impersonate you online or otherwise use services without your approval. For more information about COPPA, visit www.onguardonline.gov.

Social Networking and Tweens, Teens, and Young Adults. Social networking sites, texting, and mobile apps are increasingly important ways for tweens, teens, and young adults to socialize online. Consider speaking with your older children about what information they disclose and the risks, as well as the benefits that come from such disclosures. Sensible privacy practices may be a good defense against cyberbullying and online predators, and can also keep your child from damaging his or her long-term reputation.

Build and Protect Your Children's Digital Reputation. From an early age, parents need to encourage their children and teenagers to think about what they want their digital reputation to be. Their digital footprint is often permanent, and children need to be taught that anything they post online could be impossible to later delete. Something shared on a social network at the spur of the moment can be discovered years later by friends or prospective employers. Teens often think about how they portray themselves online to their friends, but may need to be reminded about the audience of employers, colleges and others.

Resources. There are a number of tools to help parents talk about, and kids learn about, privacy:

- The Maryland Attorney General's Office offers resources for talking to teens about social networking and Internet safety at http://www.oag.state.md.us/children.htm.
- The Family Online Safety Institute has an Internet Safety Contract and provides a number of tips for parents to consider at www.fosi.org.

- Common Sense Media provides a number of Internet privacy tips and guides on its website at www.commonsensemedia.org/advice-for-parents/internet-safety-and-privacy

Domestic Abuse or Dating Violence Survivors. Safety planning is critically important for victims of domestic or other sexual violence and abuse. Abusers may sometimes harass, stalk, or monitor survivors using technology. Some general safety tips on technology are listed below. If you want more information, ***use a safe computer or phone*** and contact the National Domestic Violence Hotline at 1-800-799-7233 or www.nnedv.org/safetynet.

Find a Safe Computing Device. If you think you may be monitored on your home computer, be careful how you use it. It is not possible to delete or clear all the "footprints" from your computing or online activities, so if you're using the computer to visit websites or do other things that might endanger you if the abuser finds out, try using a safer computer, tablet, smart phone, or device, such as a computer in a public library or at a trusted friend's house.

Using Online Accounts. On the safe computer, change your user names and passwords for sites and accounts you visit frequently. It is safest to create brand new accounts for email and new user names. Importantly, in case the unsafe computer is being monitored, you should only use these new names and passwords on the safe computer.

Email & Instant Messaging. These are not very safe or confidential ways to talk if you are in danger. It is usually safer to call a hotline from a safe phone.

Cameras in Your Computer or Tablet. If your computer or tablet has a built-in web camera, consider disabling the camera when you aren't using it, or covering up the camera with a piece of removable tape.

Smart Phones and Other Mobile Devices.

Get a new cell phone if you suspect yours is being monitored. A pay-as-you-go phone is an inexpensive alternative, or you may be able to get a donated phone.

Put a ***passcode*** on your (new) phone. Don't let the abusive person access it, in case he wants to snoop on your calls and Internet usage or load location-tracking software on it. And, once again, make sure your location and Bluetooth settings are turned off and stay off.

Turn off Bluetooth and location access. These devices can be used to locate you, so you should turn off Bluetooth and location access. You should also get rid of any smart phone apps that you do not use or do not know what they do. If your battery gets drained very quickly, this might be a sign that a program to monitor you or your location is constantly in use on your phone.

Online Privacy Rights under Maryland and Federal Law

Below is a brief summary of the state and federal laws protecting your online privacy rights.

Maryland State Privacy Laws. Maryland has several laws that work to protect your online privacy. For example, the *Maryland Consumer Protection Act* (http://www.peoples-law.org/node/508) protects consumers from unfair and deceptive acts and practices, whether they occur online or offline. This law generally prevents companies from hiding important facts or falsely representing the facts related to consumer goods, services, property, or credit in Maryland. If you think someone is violating your rights under this law, you can call the Attorney General's Consumer Protection Division Hotline at (410) 528-8662 or 1 (888) 743-0023. You may file a complaint at http://www.oag.state.md.us/Consumer/complaint.htm. If you have been damaged, you also have the right to sue the company that violated your legal rights in court.

Maryland law also requires that certain sensitive personal identifying information, such as your Social Security number, must be kept securely. *The Maryland Personal Information Protect Act* (http://www.oag.state.md.us/idtheft/businessGL.htm) requires that this information must be reasonably protected. This law also provides guidelines for letting you know if there has been a "data security breach," which means that your information was exposed to someone without permission to see it.

Finally, Maryland law protects you from having to give an employer a password to a personal account. The recently-passed *Maryland User Name and Password Privacy Protection and Exclusions Law* (http://mgaleg.maryland.gov/2012RS/chapters_noln/Ch_233_sb0433t.pdf) says that Maryland employers may not "discharge, discipline, or otherwise penalize" employees or job applicants for refusing to disclose a password or provide access to a personal account. This also means employers may not make hiring decisions on the basis of your refusing to tell them a personal password.

Lastly, Maryland offers a tool called the Identity Theft Passport, administered by this office, that helps consumers resolve financial issues caused by identity theft, and to help prevent a wrongful arrest if a thief uses your personal identifying information during the commission of a crime. More information about the Passport program is here (http://www.oag.state.md.us/idtheft/IDTpassport.htm), and you may download an application by clicking here (http://www.oag.state.md.us/idtheft/IDT_Passport_App.pdf). A new state law passed in 2013 also allows parents and legal guardians to place a security freeze on their minor child's credit records that would prevent identity thieves from opening credit accounts in the child's name.

Federal Online Privacy Law. In addition to Maryland law, federal law also protects your privacy while online and on mobile devices. In general, federal law has different, specific privacy laws for different personal activities or categories of information. Some laws deal with financial privacy and credit reports, like the Gramm-Leach-Bliley Act (GLB) and the Fair Credit Reporting Act (FCRA); some deal with health information privacy, like the Health Insurance Portability and Accountability Act (HIPPA), and others address criminal history, education information, and employment records.
The most prominent agency in U.S. privacy regulation is the Federal Trade Commission (or FTC). The FTC is in charge of preventing unfair and deceptive practices in interstate financial dealings for most companies. If a nationwide company violates the terms of its privacy notice, for example, the FTC might take legal action. You can file a secure complaint online at https://www.ftccomplaintassistant.gov/, or call the FTC's toll-free helpline at 1-877-FTC-HELP (1-877-382-4357). For more information, visit www.ftc.gov.

Other federal agencies preside over other types of conduct or information. Some examples of agencies that enforce federal privacy rights are the Federal Communications Commission (FCC), the Department of Health and Human Services (DHHS), the Department of Education (ED), the Equal Employment Opportunity Commission (EEOC), and the Department of Justice (DOJ).