INFORMATION EXPOSED

Opt Out Online

Finding & removing personally identifiable information found on the Internet.

Cynthia Hetherington, MLS, MSM, CFE, CII
Founder & President, Hetherington Group

World of Connected Devices Solved

Understanding the risks of smartphones and IoT devices.

Amber Schroader
Founder & President, Paraben

June 2020 >> Version 1.0

Hg HetheringtonGroup

paraben® corporation paraben.com

Table of Contents:

Table of Contents (continued):

Section II –The Internet of Things

About Hg

www.hetheringtongroup.com

With over twenty-five years of global experience in open source investigations and one of the first investigative firms to conduct online social media investigations, Hetherington Group develops advanced Internet investigations unique to our clients' needs. With hyper-focus and scientific precision, Hg's seasoned professional analysts scour social media networks, local media, individual public record and government databases, and Internet open sources to protect personal data in this expansive and ever-changing environment.

Hetherington Group leads in online and social media investigations, having trained over 180,000 corporate security professionals, attorneys, accountants, auditors, military intelligence professionals, and federal, state, and local agencies in Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT). Our dogged pursuit of knowledge and efficacious reporting are driven by abilities our investigators have honed for years.

Twitter: https://twitter.com/HetheringtonGrp
LinkedIn: https://www.linkedin.com/company/hetheringtongroup
Instagram: https://www.instagram.com/hetheringtongroup/
Facebook: https://www.facebook.com/HetheringtonGroup/

Contact:

400 Ringwood Avenue
Wanaque, NJ 07465
973.706.7525
cs@hetheringtongroup.com

About Paraben

www.paraben.com

Paraben Corporation was founded in 1999 as a technology design firm in 2001 Amber Schroader took over as the CEO of the organization and turned the focus of the firm to be digital forensics and cyber. As part of the focus, the last 20-years Paraben and its leadership have been watching and keeping pace with the digital frontier and the changes that have been occurring. From the release of the first tool to deal with mobile forensics in 2001 to the first technology to collect from IoT devices in 2010, the perspective on technology and the shifts in the data is at the forefront.

Amber Schroader has been in the digital forensic field for thirty years and has seen the evolution of change from just processing computers to processing smartphones to now working with IoT devices. From designing procedures to dealing with these devices as evidence and building awareness of security issues the field. As the leader of Paraben Corporation, she has taken this knowledge and spread the value of understanding your digital fingerprint to people all over the world.

Twitter: https://twitter.com/parabencorp
LinkedIn: https://www.linkedin.com/company/paraben-corporation/
YouTube: https://www.youtube.com/user/ParabenForensics
Facebook: https://www.facebook.com/parabencorp/

Contact:

39344 John Mosby Hwy Ste 277
Aldie VA 20105-2000 USA
801.796.0944
sales@paraben.com

Introduction

Surveillance is like gravity. You notice it every now and then but are mostly unaware of its ever-constant presence penetrating all walks of life, in all areas. Technology today invades every nook and cranny of our lives. Even if you consider walking through a vast forest—free of wires and Wi-Fi—there are satellites circling the earth that can zoom in and capture the reflection of your loved one off your sunglasses. That reflected image can be run through facial recognition software, and that image can be named. No one is free of surveillance, so understanding how to be an aware citizen and maintain a sense of privacy, certainty, and independence is important.

As gravity is necessary to sustainability, surveillance also has a place in today's world. Government and business reactions to COVID19 have demonstrated that technology, surveillance, and other AI have helped to slow the spread, saving millions from suffering. As Nicholas Wright wrote in Foreign Affairs:

> The novel coronavirus pandemic is causing tens of thousands of deaths, wreaking economic devastation, leading to lockdowns across much of the world, and upending societies and their assumptions. But going forward, one of its most significant legacies will be the way that the pandemic dovetails with another major global disruption of the last few years—the rise and spread of digital surveillance enabled by artificial intelligence (AI).[1]

Concern for health overrode many of the government's privacy and security protections to help, cure, or mitigate ailing people. HIPPA and other compliance were cavalierly shuffled aside to get telemedicine up and running.[2] Stranded passengers left in foreign countries gave their documents to strangers—anyone who could help—in order to facilitate their return to their home country. Business owners and the desperate unemployed filled out numerous forms in order to get financial aid—many on antiquated or unprepared computer systems—filled with security vulnerabilities.

As the pandemic settles down and society rolls into a new normal, the data we shed during the initial frenzy of COVID-19 is now out there, leaving us vulnerable. What will happen to the personally identifying information, and how can we anticipate the fraudulent or dangerous use of information and ourselves? You cannot avoid surveillance, just like you cannot deny gravity, but there are measures you can take to protect yourself and your family.

Protection means understanding that in this often confrontive and divided world, opportunists, frauds, and enemies will take advantage to undermine their target: They'll gather home addresses in order to stalk or threaten families at home, organize protests on your front lawn, terrorize you in your own house, or even worse.

Anti-establishment hackers are joining the ranks of the Crips, the Bloods, and the Hells Angels. They are opposed to the conventions of economic, social, and political principles and values of our democratic society. In the age of COVID-19, U.S. anti-government militia groups have zigzagged across Facebook, organizing for a 21st Century Civil War.[3] Advocates of this worldview would sooner see you and your family suffer than be subjected to another day of Western idealism, American justice, and democracy. A protesting, anti-government, non-conforming anarchist is welcome in America; however, once the line of civil disobedience crosses over into crime, we Americans must fortify ourselves to do our jobs and protect our families

> » You cannot avoid surveillance, just like you cannot deny gravity, but there are measures you can take to protect yourself and your family.

Section I of this report, Hg's Opt Out Online, will help you understand the dark side of information sharing. You will learn the pitfalls of oversharing and how to reduce your online risks. Section II of this report, Paraben's The Internet of Things, will help you understand connected devices and best practices for ensuring your security. Appendix A offers useful tips for protecting your personally identifiable information and preventing identity theft. Appendix B instructs on how to opt out of online vendors. Appendix C provides steps to remove your personally identifiable information from three major DNA collection retrieval services.

In this digital era, protecting personally identifiable information is of utmost importance. This report is meant to help facilitate your personal privacy in a very open online world. There is no one solution, no one vendor, that has all the answers. The best security practices start at home. Using this report as a guide, you can begin to remove, obstruct, or obscure the open source information that leaves you and your family vulnerable online.

We appreciate the opportunity to share with you Hg's tried methods to minimizing your risks while still enjoying the wonders of the World Wide Web.

Cynthia Hetherington, MLS

Cynthia Hetherington, MLS, MSM, CFE, CII
Founder & President, Hetherington Group
May 12, 2020

Amber Schroader
Founder & President, Paraben
May 12, 2020

INFORMATION EXPOSED

SECTION I

Opt Out Online

Finding & removing personally identifiable information found on the Internet.

Cynthia Hetherington, MLS, MSM, CFE, CII
Founder & President, Hetherington Group

June 2020 >> Version 10.0

> » We generate a good deal of the information found in online databases due to our inclinations for simplicity, discounts, and connectivity.

I How Much of Me Is Out There?

Data, at its most annoying, is a commodity with social media sites selling your Likes to data providers. Data, at its most dangerous, allows terrorists and scammers—as near as your neighbor or from faraway lands—to farm from open sources the personal addresses of our military personnel to threaten them and their families. They robocall mercilessly and prey on the elderly. Unfortunately, we share much of the data that generates these annoyances and threats.

We generate a good deal of the information found in online databases due to our inclinations for simplicity, discounts, and connectivity. For instance, does your keychain look like holiday garland with commercial value cards dangling from it? Gliding through the airport, do you advertise who you are with easily visible bag tags displaying your status and address? Are you or your family members regularly checking Facebook and Instagram feeds from a smartphone or a laptop? Is your wallet bulging with credit and/or debit cards and not dollars? Do your home and cell phones receive unsolicited offers or scam calls? Is your postal mailbox full of unsolicited offerings? If any of these scenarios applies to you, you are oversharing your information.

Want to get a sense of how much information you generate and spread during an average day? Try the following offline example: Over the course of a week, keep a journal of all the times you share your name, address, phone number, or credit card number on- and offline. How often you drive a car through a tollbooth with an automated payment system such as E-Z Pass or Fast Pass? How often you Like your friend's social media posts? How often you use a grocery store coupon card? How often you pay your bills online? How often you answer unsolicited email?

> » For instance, does your keychain look like holiday garland with commercial value cards dangling from it?

After this exercise, you may think that completely removing yourself from the online world would be insurmountable. Paying for goods and services with a credit card, automated toll stations, and having a minicomputer, i.e., your mobile phone, in the palm of your hand are some of the practical, modern conveniences you rely on almost daily. Give them up? Not likely.

Oddly enough, such personal information has always been readily available—although it required investigative experience and/or a serious commitment to locate these types of details through county courthouses, administrative offices, and other public record venues. Since the advent of the easily accessible and always available World Wide Web, public record companies have become accessible to everyone, with over 100 such companies in the U.S. alone. These companies will locate individuals and share personal details about where they live, who lives with them, their ages, and so on, for anyone interested in finding out.

> » The rental or exchange of customer files has been a common practice for decades and does not pose a security risk to you.

II How Is My Information Being Shared & Used?

Organizations use information from a variety of sources for a variety of reasons. You are familiar with some of them: Businesses wanting to send you an offer and companies wanting to better understand their marketplace or to develop new products and improve customer service. In other cases, companies use information to protect you and themselves from risks related to identity fraud.

Most companies rent or buy lists of individuals they believe are likely to be interested in their products or services. They will use these lists to market to you either offline or online. These lists come from a variety of sources, including public records, telephone directories, and from companies who exchange or rent their customer files for marketing purposes to other organizations who have a legitimate need for the information. The rental or exchange of customer files has been a common practice for decades and does not pose a security risk to you. The exchange usually involves only the basic contact information and very general information about your purchases. These lists are used to send postal mail and email to you, phone you, and/or text you about special promotions or offers. Contacting you in this manner enables a company to engage more effectively with individuals who are not yet customers, but who might have an interest in or need for their product or service.

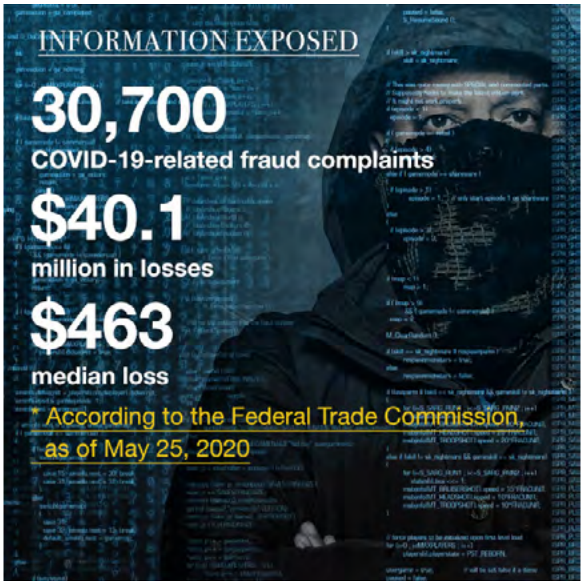
It is also common practice for a business or organization to create a marketing file of names, addresses, and other information related to their customers' purchases. Marketing data may include household characteristics obtained from surveys you fill out or from general communication with you.

Marketing, however, is only one use for your information. Early detection and prevention of fraud by verifying your identity is a second use that offers significant benefits to both you and businesses. Being able to correctly recognize a customer—especially when transacting business over the phone, on the Internet, or via a mobile device—can help reduce the chances of that customer becoming a victim of identity fraud.

There are still other uses of personal information you may not have considered, such as courts tracing parents who fail to meet child support obligations, or investigators conducting background checks for the purposes of compliance and anti-fraud initiatives, or law enforcement agencies apprehending criminals, or attorneys searching for missing heirs, or family members looking for lost relatives, to name just a few. These suggested uses provide significant benefits to society and are permitted—even, in some cases, required by various laws, such as background screening for childcare center employees and school bus drivers.

III What Kind of Information Is Available?

A variety of information is available to businesses and organizations. While most of the information is non-sensitive, some of it can be sensitive.


INFORMATION EXPOSED
30,700
COVID-19-related fraud complaints
$40.1
million in losses
$463
median loss
* According to the Federal Trade Commission, as of May 25, 2020

Public Records

Collected primarily from state and federal government sources, information about you may come from public records, including property deeds, marriage and professional licenses, and birth and death records. Information is also available from other public records such as court proceedings, voter registration files, driver's license records, and motor vehicle registrations. Note that various federal and state laws place restrictions on the use of some of these sources.

Publicly Available Information

Some information is considered in the public domain, i.e., anyone has access to it. This type of information includes telephone directory listings, professional registries, classified ads, information posted online in chat rooms, on blogs, and in public sections (or areas designated as public) on online social network sites. Publicly available information is not always regulated by law, but responsible providers self-regulate its use through industry codes of conduct.

Customer Information

Customer information is collected when you provide details about yourself to an organization when you inquire about a product, donate, make a purchase, register a product warranty, or receive a service. The detailed information you provide can include how to contact you, and a record of your interactions with the company or organization. In some cases, this information is regulated by law, and, in other cases, by industry practice. It is worth noting responsible organizations develop their own policies to assure appropriate use of the information.

Self-reported Information

Information you voluntarily provide on a survey or questionnaire is considered self-reported. When this type of information is collected, you should be informed of the intended uses and your options for said use. Both law and industry practices limit the use of this information.

> » Sensitive information should be kept confidential and is usually not provided to other organizations unless you give specific permission or unless it is permitted, or required, under state or federal law.

Passively Collected Information

The Internet and other technologies, such as mobile devices with location tracking features and interactive televisions, may collect information about you or your device without you taking any action. In fact, in many cases you may not be aware any collection takes place. Some of the collection is necessary to provide you a service, such as recording the number of times you go through the express lane of a tollbooth so you can be charged for the toll, or when you have had a car accident and emergency assistance needs to locate your car to send help. The collection of information can also be used to provide you relevant advertising, such as offering a discount on a specialty coffee from a coffee shop you are near or to provide online advertising tailored to interests that have been identified based on other Websites you recently visited or keywords you recently used in a search. Both law and industry practices limit the use of these types of information.

Personally Identifiable Information (Sensitive)

Some information, if used inappropriately, can have more serious consequences. This type of information includes your Social Security number, driver's license number, medical records, wage and salary information, tax reports, credit reports, and any information that personally identifies your children. Sensitive information should be kept confidential and is usually not provided to other organizations unless you give specific permission or unless it is permitted, or required, under state or federal law.

To develop credit reports, credit reporting agencies gather information from banks and other financial institutions with which you have a relationship. Employers, landlords, and insurance companies may ask your permission to perform a background check. This activity involves verifying the information you provided on your application with the source of the data. Background checks can also involve obtaining a credit report, if your financial situation is pertinent to the employer or landlord.

To protect consumers from potential fraudulent activities, the Federal Trade Commission closely regulates the use of this sensitive personally identifiable information as directed by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA). In 2018, the European Union enacted the Global Data Privacy Act (GDPR). This overarching legislation has had a tremendous impact on privacy laws and practices. It regulates the transfer of personally identifiable information from and into Europe—essentially blanketing all data transmission globally.

IV Four Vigilant Ways to Protect Your Privacy

Despite the overabundance of information shared and sold on the Web today, several measures for protecting your information are available to you. Commit to learning about these important protections and how to exercise the options offered to you. These four actions can go a long way in ensuring that you have enacted an ongoing course of action that will protect your privacy.

A. Read Privacy Policies

Reputable companies, such as financial institutions and credit card issuers, will often have a Privacy Policy informing you of what information the company collects and maintains, how it is used, and when it is shared with other parties. You can view the Privacy Policy of most companies on their Website or by contacting the company and asking for a copy. Companies which do not post or provide a Privacy Policy should be given extra scrutiny.

B. Choose Opt Out Options

Most companies will offer some choices regarding the use and dissemination of your personal information. Some of these choices are buried in the small print of Websites or mailers, so you will have to look for them. You should be given a chance to opt out of third-party shares by requesting that the company not provide your information about you to third parties for marketing purposes. Look for the annual statement from your credit card company that discusses the opt out options and act on them.

» Companies which do not post or provide a Privacy Policy should be given extra scrutiny.

C. Annual Monitoring for Accuracy

Organizations should maintain appropriate procedures that ensure your information for important or substantive decisions is accurate. If you feel it may be inaccurate, you should be able to access such information and have erroneous information corrected, updated, or removed. Retrieving your credit report on a regular basis and verifying the details is a good method for monitoring your private information.

AnnualCreditReport.com is a government recommended credit reporting service, and the only credit report source authorized by federal law. It provides a free annual credit report from one or all of the three national consumer reporting companies: Equifax, Experian, and TransUnion.

There are three ways to obtain this free report:

1. Order the report online: www.annualcreditreport.com;
2. Call toll-free: 877-322-8228;
3. Download an Annual Credit Report Request Form[4] and mail it to:

   Annual Credit Report Request Service
   P.O. Box 105281
   Atlanta, GA 30348-5281

D. Removing Personal Information Found Online

When you come across personal information such as a postal address, family member's name, personal account information, or social media posts naming you and your family on the Internet—and you are bound to—it is time to start opting out of online public records databases.

There are hundreds of online vendors whose sole business is aggregating public records. In Appendix B of this white paper, you will find the leading vendors in the public records business and the information needed to opt out of their service. In the event you find your personal data on other public records sites, start by searching the site for "opt out" or "data privacy," often located at the bottom of the Website's first page next to the legal statements. Because of the GDPR and other national and international laws, most Websites offer an easy online removal request form.

It must be noted, however, that not all sites are responsive, standing on ceremony that they are sharing “already public information” and don’t have to remove your data. The best approach for hard to reach sites is a calm approach: Explain that you wish to have your personal data redacted from their Website, as you did not agree to participate in their profiting from your address and personally identifiable information. There are some sites that simply will not answer your requests, which can be incredibly frustrating. No blanket law or procedure works in these instances, and each needs to be handled and considered moderately, as you are trying to get the publisher to remove your private information. Our approach has been mostly successful, but even our team faces an occasional unwilling participant. In those instances, you should contact us for guidance.

V Protecting Yourself Online

This report was not written to create panic or fear in the reader as much as it is a wakeup call to arm yourself against fraudsters, security breaches, and cyber-bullies. In the following sections, we provide insight into the best approaches to thwart identity theft, use social media safely, and how to address the popularization of DNA registries. Finally, we provide a X-point list on how best to shore up your personally identifiable information with simple, effective steps we, as cyber intelligence investigators, use when seeking to protect our clients.

VI Identity Theft

Let’s take a moment for a bit of history: The Internet began as research commissioned by the United States government in the 1960s to build a communications network that would survive a nuclear attack. By the 1980s, the precursor interconnected regional academic networks and gave way to the modern Internet. During the early 1990s, the Internet saw continued exponential growth as business, personal, and mobile computers of the general public logged on to it. Nearly everyone became an active, engaged Internet user.

> » With malware and viruses so covertly blended into today’s modern communications tools, even a software engineer might get duped into identify theft from the most benign looking email.

Nowadays everyone is online. Just as there are good and not-so-good people in the physical world, there are also good and not-so-good people in the online world. With ubiquity and facility come threats and need for caution.

Losing your identity to online theft is a serious—and all too common—concern. With malware and viruses so covertly blended into today's modern communications tools, even a software engineer might get duped into identify theft from the most benign looking email.[5]

It is incongruous that we fear identity theft from online financial services, e.g., our credit card and bank accounts, yet we disregard the risk of identity theft through our social network profiles. In truth, the established online financial and commerce systems are some of the most trusted sites available, using multi-layered encryption software to protect our financial transactions. Of course, no one system is impenetrable, but why would a cyber-thief choose to battle multi-layered encryption software to steal your credit card information when the open Internet offers up much more easily attainable information?

» A full name (even maiden name), date of birth, and current home location gleaned from an open social network account are sufficient data points for a thief to start creating a fraudulent profile.

Today, an identity thief need only turn to the personal profiles posted in social network sites, such as Facebook, Instagram, and LinkedIn, to capture key information about a targeted individual. A full name (even maiden name), date of birth, and current home location gleaned from an open social network account are sufficient data points for a thief to start creating a fraudulent profile. In fact, LinkedIn—the professional's social network workhorse—holds a veritable goldmine of personal information for identity thieves.

Consider this: LinkedIn requires users to post schools attended and jobs held with corresponding dates. Now, layer on the personal details gleaned from LinkedIn-linked colleagues and friends in the network and you can rather easily crib together a good list of controlled answers for most challenge questions—those security questions used to prompt for a forgotten password.

It is possible that you could lose access to your personal Web-based email account simply because an identity thief was able to hijack the account by answering the security challenge question. After gleaning the information from open source search engines, or from unprotected social network profiles, the security challenge question can be mere child's play for a savvy identity thief.

Should you find yourself discovering the Internet's dark side of personal identity theft, do not pack up, shut down, and remove yourself wholesale from the online world. Instead, alter or completely delete your pertinent information (i.e., date of birth, hometown name, identifying photos, etc.) from your social network profile. Edit the profile before deleting it, so the Internet crawlers will capture misinformation, not accurate information, for the caching servers, including Google and others.

VII Social Media: The Enemy in Your Home?

Reconnecting with old friends, networking with colleagues and clients even finding long-lost loves, are now all real possibilities with information from social networks accessed on desktop and laptop computers or cell and smart phones on a global scale. No extraordinary efforts and, more importantly, no extraordinary talents or intelligence are necessary. With plug-and-play social network applications, you simply fill in the blanks to answer a few questions, and you become part of a global network.

In the past, when Websites were developed and maintained by a select few, those unique participants were the only authors of what happened online. That which was once a medium for the few is now an open market for all users–good, bad, indifferent, and sometimes downright ugly. Today, anyone can share thoughts, opinions, and photos online through easily accessible social networks. And they do.

But often with ease-of-use comes lack of control. While people are reuniting, connecting, and sharing in online social networks, the dark side is also online–fomenting a space in which pedophiles are viewing the Instagram images of children, gangs are tweeting amongst one another, ISIL is recruiting, and criminals are trolling for target homes to rob as owners announce on their social networks, "We're on vacation this week!"

> » That which was once a medium for the few is now an open market for all users–good, bad, indifferent, and sometimes downright ugly.

Everyday millions of people, once content surfing the Web and emailing their friends, are now using social tools such as Instagram and Twitter to keep everyone apprised of their day-to-day lives, often in the most minute details.

Online technology has also reached the young and innocent among us who easily and readily adapt to new technologies. Their physical-world lives are also their Internet lives–with no filter. Young users can say and do pretty much anything online, and often do. On the other hand, adults and seniors also participate on online social media networks; but, unlike the younger set, these more mature folk, who grew up in an era of discretion and modesty, are not as open in their online social network postings. In general, younger people will join social networks openly; adults will exercise some modicum of caution before sharing their lives online, despite the occasional errant CEO sending out a random, damaging Tweet or unpopular image via Snapchat.

A. Online Confessions

People connected on social networks can be exposed to the most rudimentary and personal information. These shifts can initially be unsettling for the first-time user. In the physical world, good or bad news would be shared over the telephone or spoken in person to a few close friends. It would not occur to you to walk into a local grocery store and announce to your fellow patrons that you just finished a load of laundry or that you were staying home with a sick child that day. Doing so would seem awkward and inappropriate. And, yet, in online social networks such as Facebook, it often seems like the social norm to mention these details—in fact, it can feel almost a social obligation to do so.

> » Friends don't let friends drive drunk, right? Consider taking not only the keys away from that person, but also the keyboards.

In an environment of such relatively uninhibited, open communication, it is not long before overzealous opinions, bits of rage, drunken rants, and other embarrassing entries get posted. The user could be upset, deranged, or overjoyed; and his or her natural reaction is to share the emotion—often on their social network. Friends don't let friends drive drunk, right? Consider taking not only the keys away from that person, but also the keyboards.

Sharing your thoughts and activities online is not necessarily a problem. The problem comes when users forget that everyone in their social network is reading their online post. So, when you post something in frustration about your boss, co-worker, spouse, or friend, remember that the boss, co-worker, spouse, or friend—and all their networked friends (and all their networked friends)—may also be reading your posts.

There are free resources for monitoring social media networks including but certainly not limited to Twitter, Instagram, and Reddit. String searches such as "hate my boss," "cheated on my husband," or any other such confessional phrase, can be monitored using resources such as Twitonomy.com or Google Alerts if your profile is public.

B. What Not to Do on Social Media

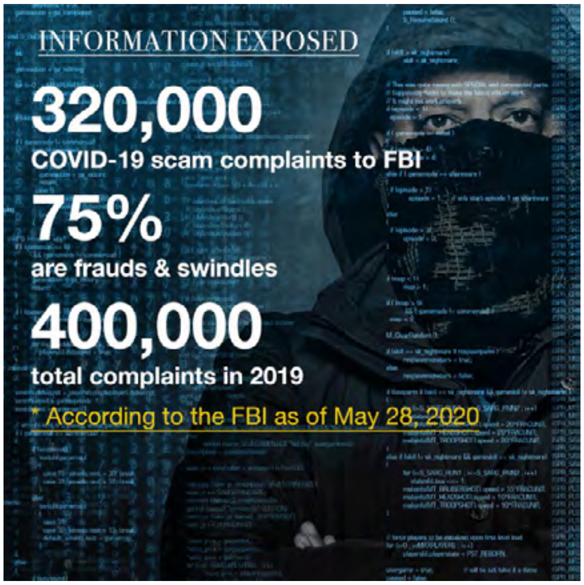
It is possible to take part in social media and still maintain a semblance of privacy. To accomplish that, keep some of the following things in mind when posting on social media platforms such as Facebook.

Do not write in a fury

If you are angry, inebriated, or simply have a big secret you are itching to share, that is the time to step away from the keyboard. What you think is hysterical or outlandish now might only serve to embarrass you later.

Do not ignore the privacy controls

Every application and online service offers customization for your profile. Use it. For example, on Facebook, limit your account access by setting who can view your posts to Friends, Friends of Friends, or Only Me. Do not enter contact information, such as your phone number and residential address. Restrict access to your photos, birth date, religious views, and family information, among other things. Give only certain people, or groups of people, access to these items, or block specific people from seeing them.



Do not post your child's name in a photo caption

Do not use your child's name in photo tags or captions. If someone else does, delete the name's tag by clicking on the Remove Tag option. If your child is not on social media and someone includes his or her name in a caption, ask that person to remove the name. Do not share online the details of your child's life. Your child's sports practice, such as soccer, is likely on a regular schedule, which a predator reading Facebook profiles can be easily track.

Do not mention when you'll be away from home

When you tell your Friends through social media that you are not going to be home, you are inviting criminals who are trolling Facebook profiles—especially unsecured profiles—to your then-unoccupied house. Keep in mind it takes only a few minutes to rob your home or harm your family. Even a mention of a quick run to the store is unwise.

Do not use a weak password

Avoid using simple names or words that can be found in a dictionary as a password. Even with numerals tacked on the end of the word, these are not secure passwords. Instead, use a knuckle-breaker password—one that requires upper and lower-case letters, in combination with numerals and symbols. A secure password should have a minimum of eight characters.

Do not put your birthday in your profile

Your birth date is an ideal target for identity thieves, who could then use the date to obtain more information about you, potentially gaining access to your bank or credit card accounts. Do not put any personally identifiable information about yourself in your social media profile accounts.

Do not let search engines find you

To help prevent strangers from accessing your Facebook page, go to the Search section of Facebook's privacy controls and select "Only Friends" for Facebook search results. Be sure the box for public search results is not checked.

Do not ignore privacy settings updates

The Terms of Service for apps and social media services changes constantly. Keep up with any notices that changes have been made to the security and third-party access permissions.

> » Being completely offline is much more suspicious than being online and oversharing every blessed detail of one's life.

Control your child's social media activity

Most young people are now using social media platforms other than Facebook, including Instagram, Twitter, Snapchat, and TikTok. Get in the habit of having your child part with his or her smart phone each night so the phone can spend the evening recharging its battery—an excellent opportunity for the parents to then peruse the contents of their child's social media profiles. Sign up for a monitoring app such as Bark, Safer Kid, or Web Watcher to monitor your children's social media activity on their phones.

Do not Friend your employer

Sure, it might seem like a great idea to Friend your boss—that is, until you decide to rant about how much you hate working overtime or you post photos of your day at the beach the same day you called sick into work.

C. Creating a Minimal Online Presence

With all the above-listed precautions, it might seem ideal to delete all your social media accounts, unplug all appliances, and move to a desolate part of the world where you can live off the grid. However, being completely offline is much more suspicious than being online and oversharing every blessed detail of one's life.

At Hg we recommend clients create a minimal online social media presence with no real valuable information attached to it. For instance, "I'm an executive in the New York metro area, with a dull life and unremarkable kids" reads perfectly as a rather benign profile that shows you have some sort of online activity. Whenever we research an individual and find no personal online information about them, their kids, family, or anyone else connected to them, we start to assume they work in the government—precisely what, if it is true, you do not want people to assume—or they are possibly dead. We would not, however, consider them gang members or drug dealers, because experience tells us those sorts of individuals love social media and are easily tracked when their accounts are found.

» So, when it comes to your social media presence, create a minimalist site with a fresh email address and no valuable content.

So, when it comes to your social media presence, create a minimalist site with a fresh email address and no valuable content. The profile image should be vague—a skyline, a piece of artwork, a picture of a favorite food, a dog, or a superhero. Do not project images with identifying marks, badges, designations, and absolutely no photos of your children. With such a profile, you might be perceived as dull online, but offline you will enjoy a larger sense of security with the ability to control your online world and the antics of those who wish to do you harm.

Cynthia's Tip

If you have been victimized by online bullying or information exposure, contact an online risk assessment company to help you discover how extensive the damage is. In the case of a local cyber-bullying attack, most victims usually have a sense of who the culprit is. However, finding out you are the target of ISIS, Anonymous, or any other anti-establishment group can be life altering for you the victim. In such cases, contact a law enforcement agency equipped to handle such concerns and a professional service firm with a solid reputation for online assessments and removals to assist you in removing any sensitive information.

The bottom line: Respect social media applications. There is an appropriate time and place for using social media. Remember, if you would not feel comfortable having your online activity broadcast through your local grocery store's public-address system, while simultaneously having a giant, neon arrow pointing directly at you, then there's a good chance your online activity has no business being online.

VIII DNA: The New Online Risk

DNA testing is alluringly attractive, because it promises to reveal hidden secrets about you. Perhaps a pedigree that has gone unnoticed, a fitness capability you have yet to try, or a predisposition for a life-threatening disease. Nothing gets closer to the core of what you are than DNA, and as luck would have it, you can access this data for $100 or less by the mail.

MyHeritage, Ancestry, Fitnessgenes, and 23andMe are ready to analyze your swab in order to tell you more about yourself. Genopalate will tell you what foods you should eat, not to be outdone by Geneticsdiet, Viome, and Vitagene. If finding the perfect mate is your query, Instantchemistry and Geneticsdigest will locate your next love. If this is all just too overwhelming for you, you can pop into the parody site, DNAfriend, to see if you are a candidate for Dutch Elm disease, reverse balding, or bad intentions.

According to BIS Research,[6] curiosity and quest have catapulted these services into a nearly billion-dollar industry. Despite the global government concerns about privacy and the overexposure of its citizens' PII, plenty of individuals are spitting in tubes and waiting on results.

A. DNA Data for Sale

> » Some companies only had policies governing use of their website, while others failed to indicate whether they strip away personally identifiable information from a sample before sending it off for testing.
> - Dr. James Hazel & Dr. Christopher Slobogin

As privacy professionals and opt out specialists, Hg sees the inherent risk to our clients who choose to swab their cheeks and send it off for analysis. Yet, an informed customer who opts not to submit his or her DNA can be exposed by a brother, cousin, or other blood relative who submits DNA. Shared DNA amongst family members creates leads and connections no one thought possible ten years ago: Today, law enforcement, genealogists, and private investigators use open source sites such as GED Match to track and trace volunteered DNA to close cold cases and find lost relatives.

It is a multi-million-dollar industry that is growing.

DNA is the latest commodity sold to companies specializing in market and product development. GlaxoSmithKline paid $300 million to 23andMe for access to the data they collected.[7] AncestryDNA sells DNA data to Calico, a Google spinoff to "Research the Genetics of Human Lifespan."[8] AncestryDNA is also the data warehouse of addresses, personal identifiers, and other key information on persons since they purchased the U.S. Social Security death index in the late 1980s. Connecting the dots between personally identifiable information and DNA has never been easier.

In a 2018 survey,[9] James Hazel and Christopher Slobogin of the Center for Genetic Privacy & Identity in Community Settings at Vanderbilt University Medical Center studied 90 DNA testing companies and found most of their privacy policies lack controls. Some companies only had policies governing use of their website, while others failed to indicate whether they strip away personally identifiable information from a sample before sending it off for testing. While a few of the larger companies may have acceptable policies, Hazel and Slobogin recommended avoiding smaller, unknown testing companies, as their privacy policies were minor to non-existent:

> We found that over 40% of companies either had no readily accessible policy documents or had policies that did not appear to govern genetic data. These "web-only" policies resembled those that might be found on any website. We saw these smaller companies that you might not have heard of had privacy policies that were a paragraph long, a couple paragraphs long, and really didn't provide any information whatsoever.[10]

The researchers also noted that the larger, more popular, and more visible companies, such as 23andMe, Ancestry.com, and MyHeritage, had stronger opt out policies in place. In comparison, however, the smaller companies could not be relied on to remove your data once in their database.

B. Be Wary of Swabbing and Sending

The experience of taking part in a DNA testing kit is advertised as exciting and fun, easy to process, and full of interesting information you may not know about yourself. The darker side of this activity is rarely discussed: You may learn things about yourself and your family you were not necessarily prepared to learn. Hg investigators have seen numerous cases of paternity questioned, familial relations discovered, and heritage probed.

» The darker side of this activity is rarely discussed: You may learn things about yourself and your family you were not necessarily prepared to learn. Hg investigators have seen numerous cases of paternity questioned, familial relations discovered, and heritage probed.

Starting the process is rather pedestrian, as DNA testing companies ask a lot of questions that may strike you as boring. However, in order to protect your data, you need to read them carefully.

As a consumer, you will want to opt out of every option that is not specifically focused on your objective such as locating your heritage. Companies like 23andMe have a separate agreement asking permission to use your DNA data in research studies. This data is stripped of identifying labels like your name or address that tie the sample to you specifically, but that is not always guaranteed to protect your privacy. Sites such as Family Tree DNA allow you to bring your results into their service for the purpose of locating more familial results. Unlike Facebook, where you look for people with the same last name and stalk them from afar, DNA is going to pattern match you to strangers you wish you never met, never mind that they are a distant relation.

Unlike Facebook you cannot unfriend them.

In their defense DNA companies, like marketing companies, strip out much of the identifying information and resell it to other marketing companies for market analytics and statistical surveys. Stripped DNA, known as de-identified aggregate data, is relatively safe. It identifies your characteristics but does not give your name or personal identifiers. All the data knows is that you are a male of Eastern European heritage with lupus indicators. This kind of data may include summaries that do not specifically call out individuals such as what percentage of people have a certain ancestry.

There have been cases where de-identified data was re-identified to the individual and used for locating specific individuals. James DeAngelo, the Golden State Killer, was identified through an open source DNA database via his relatives' DNA, as it was re-identified to DeAngelo's kin.[11] Once investigators had their names, they looked for family relations of the specific age and characteristics of the killer and found DeAngelo's blood relatives—even though he had never used a DNA test himself. A very public demonstration that even anonymized data can be used to identify people.

If you give a company permission to share your data with another research organization, you can revoke that permission later. However, it will be difficult or impossible to delete your data from third parties that have already received it. It is also hard to guarantee that those third parties will not also share your data with yet another company or research organization down the road.

The DNA testing company may also ask your permission to store your sample, allowing them to retest it again with future, advanced techniques. Some sites also offer a family finder feature that lets potential relatives contact you if your DNA matches. Reputable companies will make sure to inform you as much as possible, but be sure to read everything before you click "Agree."

C. Delete Your DNA Data from the Big Three

Since the U.S. federal government requires companies to retain DNA information in order to comply with quality control guidelines, it is never really possible to delete it forever.[12] The best way to remain anonymous is not to share a swab of your DNA. However, if you already have, you can work to have your data deleted.

Appendix C includes steps for removing as much of your data as possible from 23andMe, Ancestry.com, and MyHeritage. Each company has its own steps for deleting your data.

INFORMATION EXPOSED
90
countries in INTERPOL COVID-19 operation
4.4 Million
units of illicit pharmaceuticals seized
400,000
unauthorized & counterfeit medical devices seized
* According to INTERPOL

Appendix A

Online Protections & Identity Theft Prevention

The following tips can help you take measures to prevent your information from landing online and into the wrong hands.

» Mail: Have your postal mail sent to a United States Post Office Box or your office address. Avoid using your personal address as your business address. Business listings are much more difficult online to remove than listings for people.

» Phones: Un-list and un-publish your landline phone number. Check with your mobile service company to find out if they sell their subscribers' information and how to opt out of that list. Register all your phone numbers with the National Do Not Call Registry (www.donotcall.gov) to remove yourself from popular telemarketing lists.

» Protect Your Data: Never put your name, phone number, or personal information of any sort on any form or application without learning what the company's policy is. If you are not legally bound to enter personally identifiable information, then do not offer it.

» Financial Institutions: Mail a written request to all your credit card companies and personal banking institutions requesting your personal information be removed. Be on alert for any privacy notices mailed from your credit card vendors and insurers and read those notices. Be aware of their policies and updates to those policies.

» Credit Reports: Obtain your credit report annually and subscribe to a monthly credit agency reporting service such as Experian, Transunion, or Equifax.

» Warranty Registrations: Do not fill out and return any warranty cards. This information is resold to marketing houses, which sell to public record database companies. If you must, use an alternative address such as a Post Office box or mail drop. Alternatively, save with the original sales receipts. Provided you have both items in-hand when filing a warranty claim, the store must honor your warranty.

» Magazines: Do not use your own name or personal address for any magazine subscriptions.

» DNA Registries: Do not participate in DNA collection services, i.e., 23andme.com, myheritage.com, ancestrydna.com

» Public Records Vendors: Opt out of Public Records Data Vendors. Refer to Appendix B and follow the detailed removal procedures for each vendor. Some of the vendor sites will ask for verification of your contact information. This may seem counter-beneficial, but it is a necessary step to ensure your information is removed.

» Online Activity—Social Media & Apps

- Secure online space: Make sure all personal accounts are set to private and passwords are regularly changed. Avoid using common passwords such as family members' names, birth or anniversary dates, dog names, etc.

- Report Abuse: If someone is posting inappropriate comments about you or your family on a social network platform, report the abusive behavior to the social network's account security, e.g., the "Report" link on Facebook and LinkedIn.

- Ignore Bullies. If you come across an upsetting personal post, resist the temptation to retort. Do not reply. Antagonizing a bully will only give the bully what he or she wants: Attention. If you ignore the bully, try to contact the appropriate authorities. If you are the appropriate authority or have contacted the appropriate authorities to no avail, contact a professional service firm to assist you with the matter.

- Read privacy policies: Ensure you understand privacy policies on all e-commerce, social media sites, and apps before entering your personal information. If there is no privacy policy, this is a red flag. Avoid sharing any of your information.

» Campaign Contributions: Avoid using personal addresses for campaign contributions. Campaign donor receipts are public record and easily accessible online.

» Assets: Consider moving all current assets under a shell organization, e.g., trust fund, dba. Purchase any future assets through the shell organization, i.e., property records in your name may be public through online county databases, which are scraped and shared elsewhere online.

» Your Name: Monitor your name online. Set up Google Alerts (www.google.com/alerts) on your own name. If anything is said about you—either in a social network or elsewhere online—these services will send you a notification via email.

» Memorable Word: Tweak your memorable word (in a memorable way, of course). Come up with a surrogate word for the answers to your challenge questions. For example, if your first dog's name was Java, use the word coffee as a challenge answer and memorize that tweaked word. Or pick one obtuse word, such as rollerblade, to answer every challenge question and, again, memorize that obtuse word.

» Who's Who: If someone you have not communicated with in decades tries to contact you on a social network, ask them your own challenge question: "Hey, do you remember Jorge Beale getting stuck at the top of ropes in gym class?" The question can be honest, or you can make one up. Pay more attention to the answer—does it seem authentic?

» Discretion Knows Best: Be discreet online. Do not publish your life story on social networks. Your full name and the general vicinity of your residence are sufficient identifying information.

» Minimize Points of Exposure Online: Most importantly, do offer up mentions of Mom's deployment, Dad's late-night shift, the family vacation, soccer practice, or any other time or location sensitive information that will easily pinpoint when and where you will—or will not—be.

Appendix B

Opt Out Vendors

Web Site: http://www.accurint.com
Privacy Policy: http://www.accurint.com/privacy.html
Opt Out: Partial
Action: https://www.lexisnexis.com/en-us/privacy/for-consumers/opt-out-of-lexisnexis.page
Affiliation: LexisNexis

Web Site: http://www.acxiom.com
Privacy Policy: https://www.acxiom.com/about-us/privacy
Opt Out: Partial
Action: Acxiom offers a multiple list of products for which it buys and sells identifying information. Be sure to opt out of all of them to remove yourself from standard consumer dataservices. To locate the different product opt out pages visit https://isapps.acxiom.com/optout/optout.aspx
Affiliation: Google, Yahoo, Whowhere, and Lycos

Web Site: https://www.beenverified.com
Privacy Policy: https://www.beenverified.com/faq/privacy
Opt Out: Yes
Action: Visit the following opt-out page: https://www.beenverified.com/app/optout/search .
Enter the requested information and click search. Select the correct profile containing your personal information. Then enter an email and select 'send verification email.' BeenVerified will send a confirmation email to the email entered. Click the verification link and the record will be removed within 24 hours.
Affiliation: Backgroundchecks.org, Emailfinder.com, Peoplesmart.com, Searchpeopledirectory.com

Web Site: http://clear.thomsonreuters.com
Opt Out: Partial
Action: Follow the directions located on the following page: http://static.legalsolutions.thomsonreuters.com/static/pdf/opt_out_form.pdf
Additionally, an individual can email any questions about who can request removal of their personal information or what kind of documentation is required to: westlaw.privacypolicy@thomsonreuters.com.
Affiliation: Thomson Reuters, WestLaw

Web Site: https://infotracer.com

Privacy Policy: https://members.infotracer.com/customer/terms?tab=privacy

Opt Out: Yes

Action: Visit the following opt-out page: https://infotracer.com/optout/

Find your profile and select 'remove my data' on the right hand side of the profile. Proceed to enter an email and comment, although a comment is not necessary and click submit. Check email inbox for the confirmation email. However, if confirmation email is not found in the inbox; check your Spam folder as the email often times redirects there. Click the comfirmation button in the email and removal could take upwards of 30 days.

Affiliation: Backgroundreport360.com, CivilRecords.org, Emailtracer.com, Everify.com, Inforegistry.com, Inteligator.com, Locatepeople.org, Recordsfinder.com, Reversegenie.com

Web Site: http://www.instantcheckmate.com

Privacy Policy: http://www.instantcheckmate.com/privacy_policy

Opt Out: Yes

Action: Visit the following opt-out page: http://www.instantcheckmate.com/optout

Enter the requested informaton and click search. Find the correct profile and click 'remove this record.' Then enter an email and click send confirmation email. Instantcheckmate will send a confirmation email. Click confirm opt-out and removal could take approximately 48 hours.

Web Site: http://www.intelius.com

Privacy Policy: http://www.peopleconnect.us/privacy

Opt Out: Yes

Action: Visit the following opt-out page: https://www.intelius.com/optout

Enter the requested informaton and click search. Find the correct profile and click 'select & continue.' Then enter an email and click continue. Proceed to click the confirmation link in the email. Once comepleted, removal could take approximately 72 hours.

Affiliation: Easybackgroundchecks.com, Lookupanyone.com, Spock.com, Peoplelookup.com, Phonesbook.com, Publicrecords.com, USsearch.com

Web Site: http://www.lexisnexis.com

Privacy Policy: http://www.lexisnexis.com/privacy

Opt Out: Partial

Action: Visit the following opt out page to learn about removing yourself from several of the LexisNexis Risk and Legal products: https://www.lexisnexis.com/en-us/privacy/default.page#optout

Affiliation: Accuity.com, Accurint.com, BridgerInsight.com, WorldCompliance.com

Web Site: http://www.mylife.com

Privacy Policy: http://www.mylife.com/privacy-policy

Opt Out: Yes

Action: Send an email to privacy@mylife.com and title the email ‘opt-out.’

Locate your profile on mylife.com. Copy and paste the name, age, and city and state into your email exactly how they appear on the website.You will need the URL as well. If Mylife.com denys the removal request, respond back by sending them their privacy policy from the website, which specifies you have the right to remove your information.

Web Site: https://nuwber.com

Privacy Policy: https://nuwber.com/policy

Opt Out: Yes

Action: Start by searching for desired profile in Nuwber.com. Once desired profile is located click ‘view details.’ Copy and paste the URL to this profile page and enter the URL into Nuwber’s opt-out page: https://nuwber.com/removal/link . Proceed to enter an email and click remove. In the email from Nuwber, click the confirmation link and removal process is complete.

Web Site: https://radaris.com

Privacy Policy: https://radaris.com/page/privacy

Opt Out: Yes

Action: You will need to create an account on Radaris.com to control your information. Once your profile is created, find your profile and select ‘full profile’ button. Next, select the down arrow next to the name at the top of the profile and select ‘control info.’ Select ‘control info’ once again and then follow the instructions on the screen. Upon entering the verification code you’ll be brought to another screen where you will select ‘view profile.’ This will bring you back to the original profile and from here select the same down arrow as before and click ‘control info.’ Following this, select ‘manage info’ and then first click ‘make profile private’ and then choose “delete specific records.’ There is a limit of deleting only 6 records so choose the most important records you feel necessary. Removal is immediate.

Affiliation: Hometry.com, People-background-check.com, Rehold.com

Web Site: http://www.spokeo.com
Privacy Policy: https://www.spokeo.com/privacy
Opt Out: Yes
Action: Start by searching for desired profile in Spokeo.com. Once you find your listing, select 'see results.' Copy and paste the URL to this profile page and enter the URL into Spokeo's opt-out page: https://www.spokeo.com/optout . Proceed to enter an email and click remove this listing. In the email form Spokeo click the confirmation link and removal could take approximately 2-3 days.

Web Site: http://www.thatsthem.com
Privacy Policy: https://thatsthem.com/privacy-policy
Opt Out: Yes
Action: Start by searching for desired profile in Thatsthem.com. Go to Thatsthem's opt-out page: https://thatsthem.com/optout. Copy the information exactly as it appears in the profile into the opt-out page and click submit. If not exact, the listing will not be removed. Removal could take approximately 5 days.

Web Site: https://www.truthfinder.com
Privacy Policy: https://www.truthfinder.com/privacy-policy
Opt Out: Yes
Action: Visit the following opt-out page: https://www.truthfinder.com/opt-out/
Once you find your profile through the opt-out page search, select 'remove this record' at the bottom of the page. Enter a valid email and wait for a confirmation link to be sent to the email. Once confirmed, removal could take approximately 72 hours.

Web Site: https://www.whitepages.com
Privacy Policy: https://www.whitepages.com/data-policy
Opt Out: Yes
Action: Regular Result – Find your profile and select 'view details.' Copy and paste the URL to this page and enter the URL into Whitepages's opt-out page: https://www.whitepages.com/suppression_requests
Click the 'remove me' and select an option. Enter a valid phone number and follow the automated phone call directions to complete the removal process. Removal could take approximately 24 hours.
Premium Result - Premium profile is distinguished by its blue color and 'Premium Result' title. For removal of a premium record, follow the directions located on Whitepages.com support link: https://support.whitepages.com/hc/en-us/requests/new
Affiliation: 411.com, Emailsearch.com, Switchboard.com

Web Site: https://www.xlek.com

(*formerly Cubib.com)*

Privacy Policy: Yes, but does not redirect

Opt Out: Yes

Action: Start by searching for desired profile in Xlek.com. Once desired profile is located, click on the profile. Now on this profile, click the ‘opt-out’ option and proceed to enter the first and last name of the desired individual as well as an email for removal. Click proceed, and the opt-out process is complete.

INFORMATION EXPOSED

36%

of CNBC Technology Executive Council members have seen cyberthreats rise since work-from-home orders took effect

* According to a CNBC flash survey

Appendix C

How to Opt Out of Top DNA Databases

Web Site: **http://www.23andme.com**

Privacy Policy: https://customercare.23andme.com/hc/en-us/articles/212170688-Requesting-account-closure

Opt Out: Mostly, your DNA information will be retained for CLIA compliance.

Action: Visit your account settings page: https://you.23andme.com/user

Find the "Delete Your Data" option under "23andMe Data." You can download any or all of your data before you destroy it. If you agreed to have your sample saved, it will also be physically destroyed.

Web Site: http://www.ancestry.com/dna

Privacy Policy: https://www.ancestry.com/cs/legal/privacystatement

Opt Out: Mostly, your DNA information will be retained for CLIA compliance.

Action: Visit your account settings page: https://www.ancestry.com/dna/

Choose "Your DNA Results Summary." From there, click Settings and choose Delete Test Results. You'll have to enter your password again to confirm that you want to delete your information.

Web Site: https://www.myheritage.com/dna

Privacy Policy: https://www.myheritage.com/FP/Company/popup.php?p=privacy_policy

Opt Out: Mostly, your DNA information will be retained for CLIA compliance.

Action: Visit your account settings page: https://www.myheritage.com/dna

Click your name in the upper-right corner and choose Account Settings. From there, scroll to the bottom of the page and click Delete Account. You can also choose to delete your Family Tree Builder projects or sites without deleting your entire account, but this will not necessarily delete your data.

Endnotes

[1] Wright, N. (6 April 2020.) "Coronavirus and the Future of Surveillance Democracies Must Offer an Alternative to Authoritarian Solutions." Foreign Affairs. Retrieved from https://www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance

[2] Severino, R. (30 March 30, 2020). "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency." Retrieved from https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

[3] Tech Transparency Project. (22 April 2020). "Extremists Are Using Facebook to Organize for Civil War Amid Coronavirus." Retrieved from https://www.techtransparencyproject.org/articles/extremists-are-using-facebook-to-organize-for-civil-war-amid-coronavirus

[4] You can download the form at the following websites: www.consumer.ftc.gov/articles/0155-free-credit-reports, www.consumerfinance.gov/askcfpb/311/how-do-i-get-a-copy-of-my-credit-report.html, and www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf. Please note that the sites will ask you for personal identifiers which might seem intrusive but is necessary for you to apply for your credit report.

[5] The prevalence of online identity theft is indeed significant, but do not overlook the traditional venues—the places where you regularly use your credit card. It is sadly almost predictable how often private, financial information will likely be compromised (hacked) from point-of-sale equipment in the commercial establishments you patronize.

[6] BIS Research. (21 May 2019). "Global Direct-to-Consumer Genetic Testing Market to Reach $6.36 Billion by 2028." Retrieved from https://www.prnewswire.com/news-releases/global-direct-to-consumer-genetic-testing-market-to-reach-6-36-billion-by-2028--300853946.html

[7] GSK. (25 July 2018). "GSK and 23andMe sign agreement to leverage genetic insights for the development of novel medicines." Retrieved from https://www.gsk.com/en-gb/media/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines/

[8] AncestryDNA. (21 July 21 2015). “AncestryDNA and Calico to Research the Genetics of Human Lifespan.” Retrieved from https://www.ancestry.com/corporate/newsroom/press-releases/ancestrydna-and-calico-to-research-the-genetics-of-human-lifespan.

[9] Hazel, J., & Slobogin, C. (2018). “Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies.” Cornell Journal of Law and Public Policy, 18-18, 1-33. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3165765

[10] Hazel & Slobogin, 2018

[11] Murphy, H. (29 August 2018). “She Helped Crack the Golden State Killer Case. Here’s What She’s Going to Do Next.” New York Times. Retrieved from https://www.nytimes.com/2018/08/29/science/barbara-rae-venter-gsk.html

[12] https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/index

INFORMATION EXPOSED

SECTION II

World of Connected Devices Solved

Understanding the risks of smartphones and IoT devices.

Amber Schroader
Founder & President, Paraben

June 2020 >> Version 1.0

Contents

About Us

Paraben Corporation was founded in 1999 as a technology design firm in 2001 Amber Schroader took over as the CEO of the organization and turned the focus of the firm to be digital forensics and cyber. As part of the focus, the last 20-years Paraben and its leadership have been watching and keeping pace with the digital frontier and the changes that have been occurring. From the release of the first tool to deal with mobile forensics in 2001 to the first technology to collect from IoT devices in 2010, the perspective on technology and the shifts in the data is at the forefront.

Amber Schroader has been in the digital forensic field for thirty years and has seen the evolution of change from just processing computers to processing smartphones to now working with IoT devices. From designing procedures to dealing with these devices as evidence and building awareness of security issues the field. As the leader of Paraben Corporation, she has taken this knowledge and spread the value of understanding your digital fingerprint to people all over the world.

This report is designed to help facilitate the protection of your personal data in a connected world. There is no one solution, no one vendor, that has all the answers. The best security practices start with you and the choices you make at home.

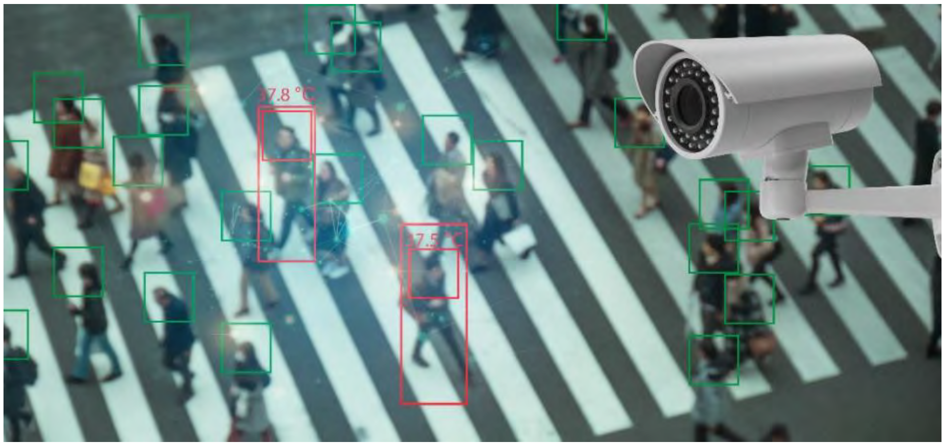
Why these devices matter

When I watched my first science fiction film, I was mesmerized looking at a world with talking robots, machines that would make any food you want, and the utopian society it helped create. What they didn't talk about in those science fiction moments is the addiction to the devices that occurred by all the people as the society turned to technology to manage their day to day lives. In the end, we have to always ask ourselves how much reliance do we want to have on our technology?

20% of people would rather go without shoes for a week than take a break from their phone.[1]

Although our smartphones act as a hub to our connected lives with it being accessed more than any other device throughout our days there are a variety of other devices that are creeping into the forefront with the more connection we incorporate into our homes, cars, and work environments.

This has become even more true with our connected devices being our connection out to the world in a time of social distancing and quarantine.   As people ramped up their connections to the digital world the data, they generated skyrocketed while their in-person connections decreased.



The other side of IoT in a pandemic is the tracking and monitoring done from drones or IoT cameras to see if people have fevers.

Kinsa Health has used data gathered from its over one million connected thermometers to produce daily maps showing which US counties are seeing an increase in high fevers.[2]

With the increased need for medical equipment and connection to multiple organizations, the answer to share data through IoT enabled devices became obvious. However, with all good innovations come to the other side of data security, privacy, and other concerns for the health and safety of our online identity.

As we explore the connected devices, we will go into what your best practices can be and how you can exist as securely as possible in this connected world.

[1] 45 Scary Smartphone Addiction Statistics, 2020 [Nomophobia On The Rise], by Deyan G. | March 18, 2019

[2] IoT set to play a growing role in COVID-19 response, April 01, 2020, Julian Watson, Josh Builta (https://technology.informa.com/622426/iot-set-to-play-a-growing-role-in-the-covid-19-response)

What are the devices?

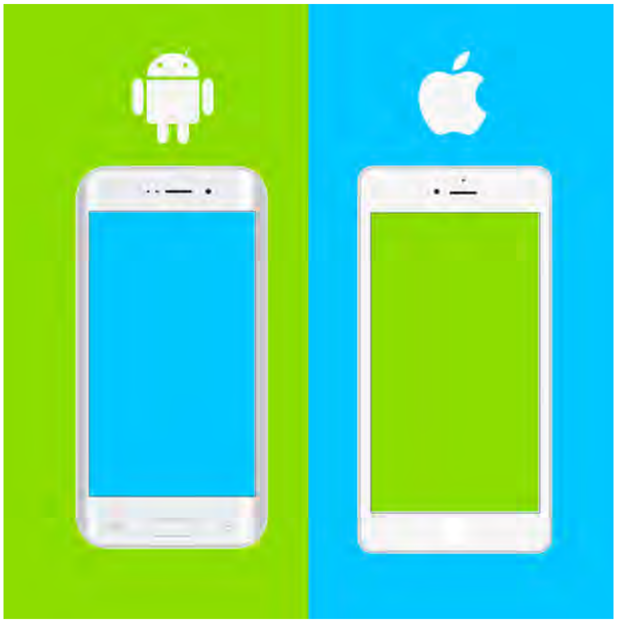
When individuals think of their digital devices there is an endless list of items they choose to connect to as well as the ones they have to connect to. The goal is to start defining the digital device spaces and where you should and should not connect.

Device Categories

When using the generic term device, it is hard to pin down exactly what you might be looking for. We are breaking the devices into two primary categories and will be addressing each of those categories in detail in each section.

- Smartphones
- IoT Devices

What is a Smartphone?



Many people feel that a smartphone is limited to the device they use as their primary mobile phone. However, if you look at the clinical classification many other devices might fall into this category.

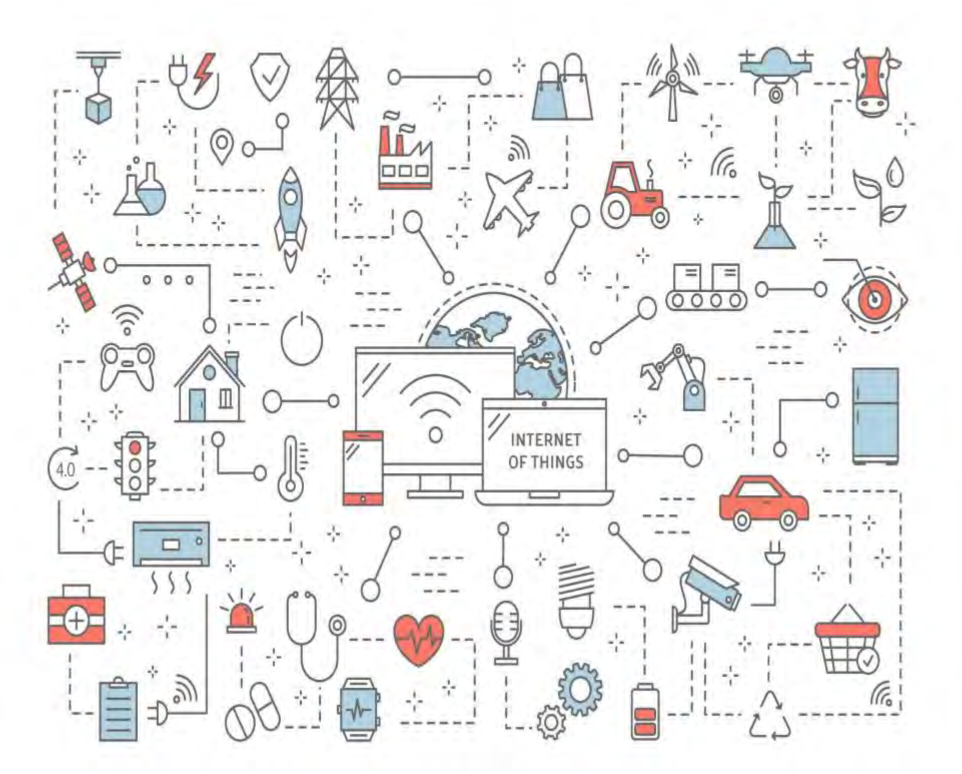
A smartphone is a small mobile device with a primary operating system that allows the addition of data interaction from a variety of mobile sources.

Within the smartphone environment, two primary operating systems exist, Apple iOS and Android. Both Apple and Android are found all over the world and many times, in the same family, with each member choosing a smart device to their personal preference. With that in mind, understanding any limitations that exist based on the type of OS preference should be noted.

With this, more clinical definition devices such as smartwatches, and even some IoT devices might fall into this "smart" category.

What is an IoT device?

The Internet of Things, or IoT, can be defined as: a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.[3]



The definition or areas might feel similar to what you expect with a smartphone. However, the key distinction of IoT is that it does not require human-to-human interaction. The design of IoT is to integrate with, and become part of, our daily lives. This is the key point to remember when you think about the different devices and their security.

Types of different devices

Smartphones

When considering smartphones, the two dominant operating systems in the world are Apple or Android. Based on the selection of the "team" you want to be on, you will have different security concerns and different controls that will need to be put into place to maximize your safety. Many times, in a single-family environment, you will have a variety of device types, with both operating systems each with potentially different OS versions. Because of this reality you need to look at each device as individually as you would each member of the family.

[3] TechTarget (https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT)

Apple Devices

On January 9, 2007, Steve Jobs announced the first iPhone at the Macworld convention. It is not a huge surprise that this handheld device received a lot of attention as it was touted as the future of technology. The first device released later that year with astounding sales and excitement by the consumer.

As time continued on the Apple device has grown in popularity and capability. With the first devices having limited interaction with 3rd party tools and only one browser to the millions of Apps of today that allow you to do just about anything you want from shopping, games, fitness, and more all from within some App in your smartphone.

Android Devices

Androids start was at a similar time but from a different perspective. The first public beta of Android was launched on Nov 5, 2007, and was developed from an operating system originally designed for digital cameras. The unique side of the Android OS is also what creates the challenges we contend with today. Android was originally launched with the Open Handset Alliance which is a conglomerate of the largest mobile phone manufacturers in the world. Their goal was to use a single operating system that could be configured and adjusted by each of them as needed. This flexible standard is what created the draw to Android but also created many more security issues. The first handset the T-Mobile G1, also known as the HTC Dream in other parts of the world came out in October of 2007.

Today, the largest issue with Android is that it is designed to exist on any variety of devices. Manufacturers can take their own spin on the firmware and change access, features, and more.

Summary

Regardless of the type of OS you are using, they both have similar issues when it comes to data sharing. The manufacturers of these smart devices work hard to maintain a competitive stance and are constantly looking at adjustments to be made to offer the next best thing to the consumer. However, that next best thing does not always keep in mind the best interests of the consumer security and keeping a mindful eye on new features before jumping in is always the safest bet.

Smartwatches

The number of wearable devices shipped worldwide is expected to double from 2019 to 2022. Shipments of smartwatches are predicted to increase by more than 50 percent over that period.[4]

The most popular smartwatch is the Apple Watch, made by Apple. This device has grown in popularity as the security limitations were cut back and new capabilities were added.

5

With the touch interface, most of the general functionality available on the primary device of the smartphone can be done from the watch screen. The key is that the watch, in the current editions, can work independently of a smartphone and contain data that that is different from the smartphone it is paired with.

[4] (https://www.statista.com/statistics/385658/electronic-wearable-fitness-devices-worldwide-shipments/)

[5] (https://thenow.ca/news/1-in-6-american-adults-is-wearing-a-smartwatch)

Fitness Bands

More than one in four Americans currently use one product or the other: 8% are actively using only a fitness tracker, 9% are actively using only a mobile health app, and 10% are actively using both.[6]

The fitness band craze has led to these devices becoming the most popular wearable IoT device in recent years. With the constant goal of the consumer public to get in better shape, this device band continuously reminds you to walk around, jump, and get moving. Today fitness bands have leveled off as the most common of the IoT devices.

As the fitness band has increased in functionality there is still one key difference between it and a smartwatch. That difference is the App access on the device. Fitness bands are still primarily run by synchronization with their individual App on another device. In contrast, a smartwatch is running the same apps that are running on the smartphone. This critical distinction shows you were you should focus when implementing security controls on each type of device.

[6] One in Five U.S. Adults Use Health Apps, Wearable Trackers, BY JUSTIN MCCARTHY, GALLUP

Home Assistants

U.S. smart speaker owners rose 40% in 2018 to reach 66.4 million with total smart speakers in use rising to 133 million[7]

"Alexa, turn on the lights." No one would have ever thought that by giving an AI (Artificial Intelligence) a name the general public would adopt these small devices and give them the same access as a member of their family. The home assistant is the next most common IoT device and the largest AI to spread through a variety of devices. With new devices coming into the market from new providers every year this area for IoT has a lot of growth to be had.

[8]There are a variety of devices available in the home assistant market to include the Amazon Echo/Alexa device in its varied form factors, Google Home, Apple Home Pod, Facebook Portal, and more. No matter who makes the device, the market for these helpful assistants is in the search market as your handsfree helper.

Whether you are working with Alexa in your kitchen as your timer and sous chef or act as handsfree in your car she is with you everywhere. The home assistant has gone beyond the bounds of the home to be an AI designed for a home user.

[7] U.S. Smart Speaker Ownership Rises 40% in 2018 to 66.4 Million and Amazon Echo Maintains Market Share Lead Says New Report from Voicebot, BRET KINSELLA, March 7, 2019 (https://voicebot.ai/2019/03/07/u-s-smart-speaker-ownership-rises-40-in-2018-to-66-4-million-and-amazon-echo-maintains-market-share-lead-says-new-report-from-voicebot/)

[8] (https://www.amazon.com/Alexa-Enabled-Navigation-Announcements-Streaming-Compatible/dp/B079FYG5TC/ref=sxts_sxwds-bia-wc-p13n1_0?cv_ct_cx=Anker+ROAV&dchild=1&keywords=Anker+ROAV&pd_rd_i=B079FYG5TC&pd_rd_r=9ab2f6a8-f70a-4436-a063-892d098c14ec&pd_rd_w=qz5Hn&pd_rd_wg=86hKC&pf_rd_p=d027eaac-7531-45fe-a61e-20ae30db06de&pf_rd_r=0XYTHS7KD51WST924PN3&psc=1&qid=1590514730&sr=1-1-70f7c15d-07d8-466a-b325-4be35d7258cc)

Home Security

As a close second to the home assistants, you can expect more and more of the home security systems to become IoT aware as they collect data from our doorbells, outdoor cameras, and even open our doors when we are not home.

The home security IoT perspective comes from a variety of different devices that are all designed to make our lives simpler, but oddly more complex as we network everything together.

While there is a lot of integration in this IoT space, the biggest concern is whether or not home security can still be done without IoT.

Children's Devices

Our children come from generations that have not known life without the internet and the idea of not being connected simply does not compute. So, what is the risks to the devices that our kids are connecting to that are connecting them.

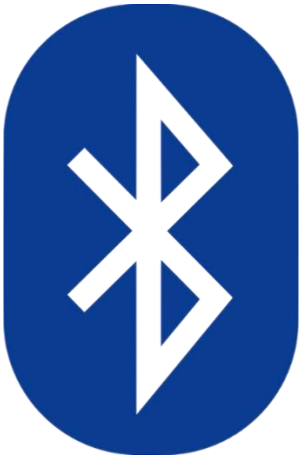
IoT toys and learning tools are on the rise. They are working their way into our children's lives as toy companions when friends are not there, or as interactive books and games. The possibilities are endless, but they can leave our kids at risk while they connect to the IoT world.

As the question of privacy comes to the forefront about children's rights, the retail force behind IoT toys is changing their approach when deciding what types of IoT toys to offer to minors when there are potential security risks.

Signals with devices

As we continue to explore the world of connected devices, one of the foundational areas we must explore is with what gives these devices life: connection. There are three primary standards devices use for connections and it is important to understand how they work, and how to secure them, to ensure we can implement and follow best practices.

Bluetooth



Is a short-range wireless communication technology that uses radio waves to transmit information, much like Wi-Fi. But where that wireless standard operates semi-permanent networks and can do so over a vast distance. Bluetooth is typically more limited and personal than that. [9]

So, in the end, Bluetooth is designed for short communication between two devices. This is why it can be key in the world of IoT where you are working in a limited physical area for connection to a device.

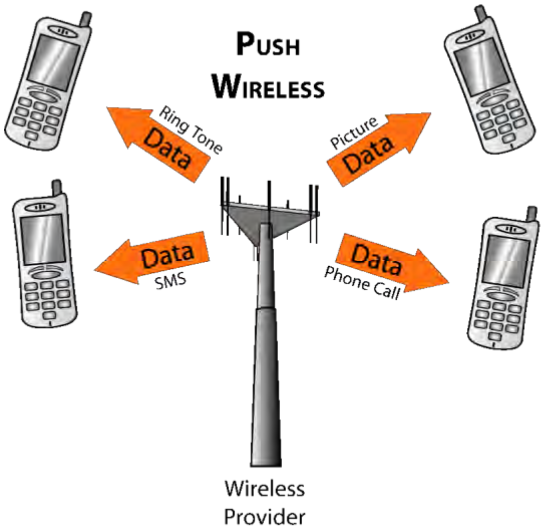
Here is a perfect example of where Bluetooth can work with another device and might go undetected in your security check. A common IoT device used by many animal loves is a tracker for their dogs. It allows them to not only know the location of their beloved animal, but it can also find out their fitness levels and create a social community with others by sharing that data to create a sense of community. A common device called a Fi is integrated into your dogs' collar for this purpose.

It is designed to connect with multiple types of connections to help you track, and find your dog if they are lost. However, in its home state, it is designed to be tethered via Bluetooth signal to the primary smartphone associated with your dog. For the device to work in its optimal setting the Bluetooth signal must be kept on to maintain the link. Although this is not a large issue in a home environment it is not uncommon for someone to forget to turn their Bluetooth off when they leave their home. This minor infraction can leave the primary smartphone that is the hub to many of the devices in your home vulnerable to attack. This is when a decision point occurs, forcing you to decide between some of the functionality of your device vs the security you desire.

[9] Why Bluetooth after this famous king, Jon Martindale, Oct 11, 2019 (https://www.digitaltrends.com/computing/what-is-bluetooth/)

Cellular Connection

Cellular is a networking technology typically associated with a mobile telephone system that uses short-range radio stations to facilitate mobile device communication over areas comprised of cells and transceivers.[10]



To simplify, cellular technology is controlled by devices that you do not control yourself. When looking at cellular from the security perspective that is the easiest perspective. With all of the smartphone type devices, cellular is typically built-in and not something that can be enhanced by the end-users since it is all about proximity to a tower. Data operates in a push function to the device. The only end-user control is through the use of Airplane Mode that allows you to isolate your device from the cellular network and exist on the other available connections such as Wi-Fi and Bluetooth.

This connection type is a have or have not there is no in-between option and with the smartphone devices, it is a have to be able to get the remote connection and to make phone calls. This connection is not as common with IoT devices as they do not require the phone call options and do not maintain a separate cellular service plan to exist at an extended distance from their home zone.

Wireless or Wi-Fi

Wi-Fi is a technology that uses radio waves to provide internet access to mobile devices such as smartphones, laptops, tablets, etc. and to facilitate intercommunication wirelessly.[11]

Wi-Fi has become a critical infrastructure in most people's lives with free Wi-Fi access in stores, coffee shops, schools, and sometimes even in friends' homes to always be connected. With all of your smart devices being able to connect via Wi-Fi the configuration and management of this primary wireless service are critical to be able to maintain your device security and the security of your data.

[10] (http://www.differencebetween.net/technology/internet/difference-between-wi-fi-and-cellular/)

[11] (http://www.differencebetween.net/technology/internet/difference-between-wi-fi-and-cellular/)

Setting up your devices

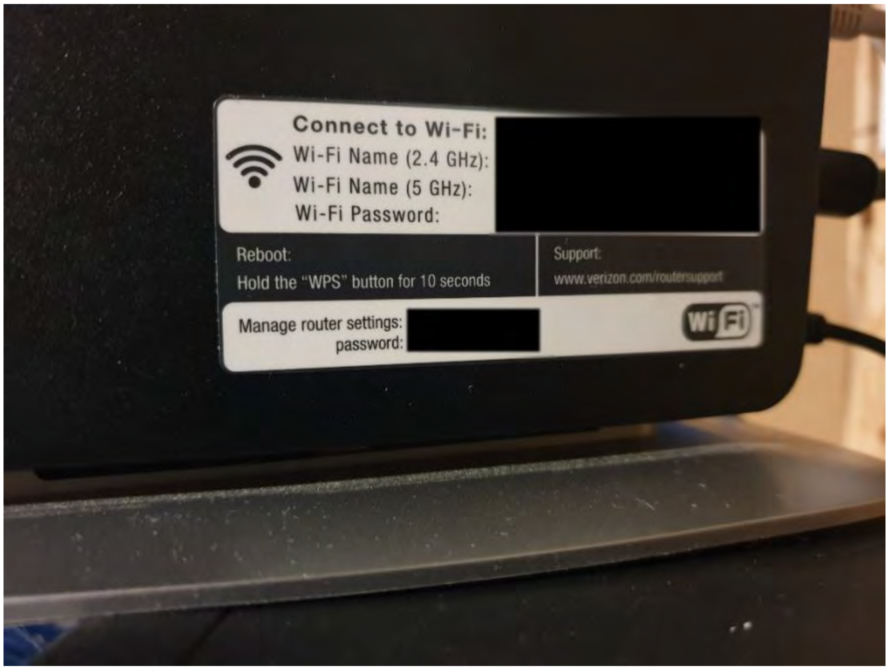
The first step in maintaining your security and protection with these connected devices starts with the initial configurations and what you are connecting to. The following are recommendations for best practices and are designed to have the balance of the use of the devices and security of the data they have access to.

Routers

Since the Wi-Fi signal is the primary data transfer option with many of the connected devices it is important to make sure that this is the first area for proper configuration. Many times, when setting up a home network you follow the recommendations of the getting started guide that comes with your router and the guidance of the provider. However, their guidance is simply for connection and not for the protection of your data.

Basic Security of Home Network

When you are setting up your home network there are a few basic things you can do to make sure you are starting with the best foot forward. First do not keep the default settings of your router. Typically, most people do not deviate from these settings and it is easy for someone to gain physical access to your router, read the credentials, and take those with them.



This is the first easy step to stay more secure by adding a new administrative account into the router with your password.

When you select a password select one that is difficult such as a passphrase like *I0Td@t@1sfun!* Or use one from one of the many password generators (https://passwordsgenerator.net/) available that are long and complex. This will make it more difficult when you forget your Wi-Fi password, but it will also make it more difficult for others to gain access to your Wi-Fi network.

Segmenting Networks

When setting up your network with IoT in mind it is extremely important to set up a separate section of your network for just your IoT devices to connect to. This of this as the front and back yard of your home. You are telling everyone the status of your home with the front yard the grass is green and mowed and you look that you have set up things well. This is seen in your wireless network by having a secure connection with nothing open broadcasting. Then we get to the segment of your backyard. You are adding a fence to that yard to obscure the details of what is back there. This is the same with a segmented network. All of your neighbors do not need to know how many IoT devices you have and what they are connecting to. If there ends up being a vulnerability it is still behind those fences you have put up and you can resolve it before the public knows.

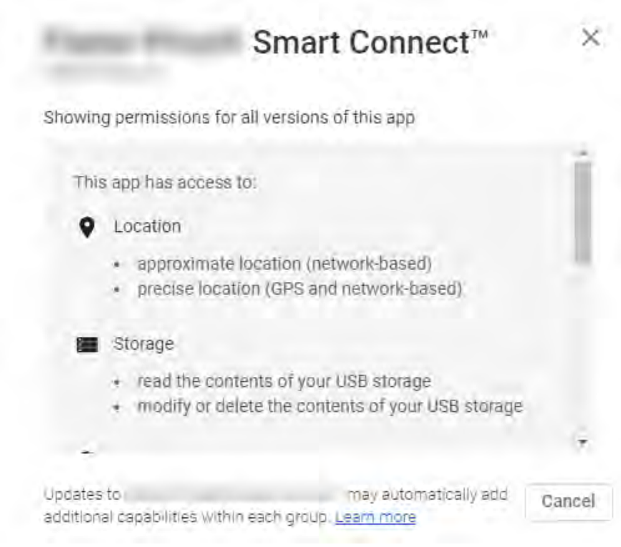
Setting up this type of network segmentation is easy and can be done through the interface of your router. Every router is different so you will have to reference back to the instructions of your router. Typically, it is recommended you get a separate wireless router for just your IoT items and have that router connect into your primary router. That creates the fence I mentioned earlier in the analogy. If something happens in that fences that have a concern then you can easily disconnect that one router with the connected devices and stop the issue from spreading to your primary network. This simple method allows you to keep the connections limited and segmented at all times for your connected devices that are smartphones and IoT related.

Identifying Options

Whenever you set up an IoT or a smart device typically you are given a lot of connection options and setting options. Although like most people you might tend to select the default options it is important to note that this might leave you more vulnerable than you might realize. By reading through and making adjustments from the default options on the device you are improving your best practices. For example, when you set up an IoT device use an email address that is not your primary address, but one specifically set up for your IoT devices. When my IoT devices connect and provide update details I can then review them through something that is not my primary email.

Permissions

With the options also comes permissions. With many Apps, they are granted permissions to different areas of your smart devices. Since most IoT devices are managed through an integrating hub such as a smartphone it is important to be mindful of the permissions that are granted to the device. By granting permissions to the App of the IoT device to things like your storage you grant it the ability to see all data from items that are from other Apps that store data there to things such as your entire gallery of pictures. It is important to watch what the App wants access to understand what the intent of the device might be beyond what you thought.



[redacted] Smart Connect™ ×

Showing permissions for all versions of this app

This app has access to:

Location

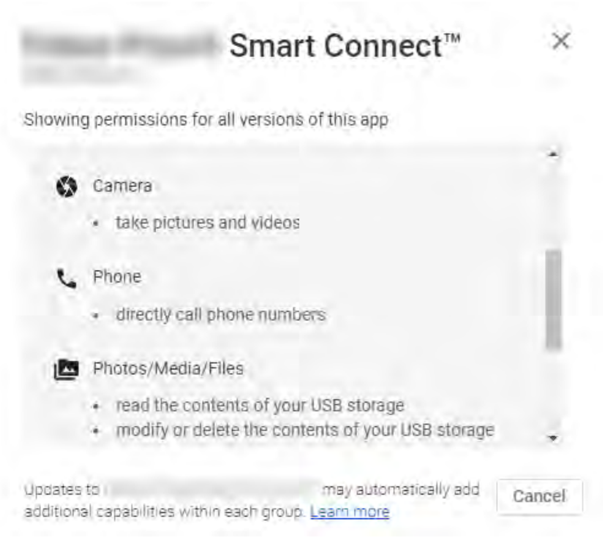
- approximate location (network-based)
- precise location (GPS and network-based)

Storage

- read the contents of your USB storage
- modify or delete the contents of your USB storage

Updates to [redacted] may automatically add additional capabilities within each group. Learn more

Cancel



[redacted] Smart Connect™ ×

Showing permissions for all versions of this app

Camera

- take pictures and videos

Phone

- directly call phone numbers

Photos/Media/Files

- read the contents of your USB storage
- modify or delete the contents of your USB storage

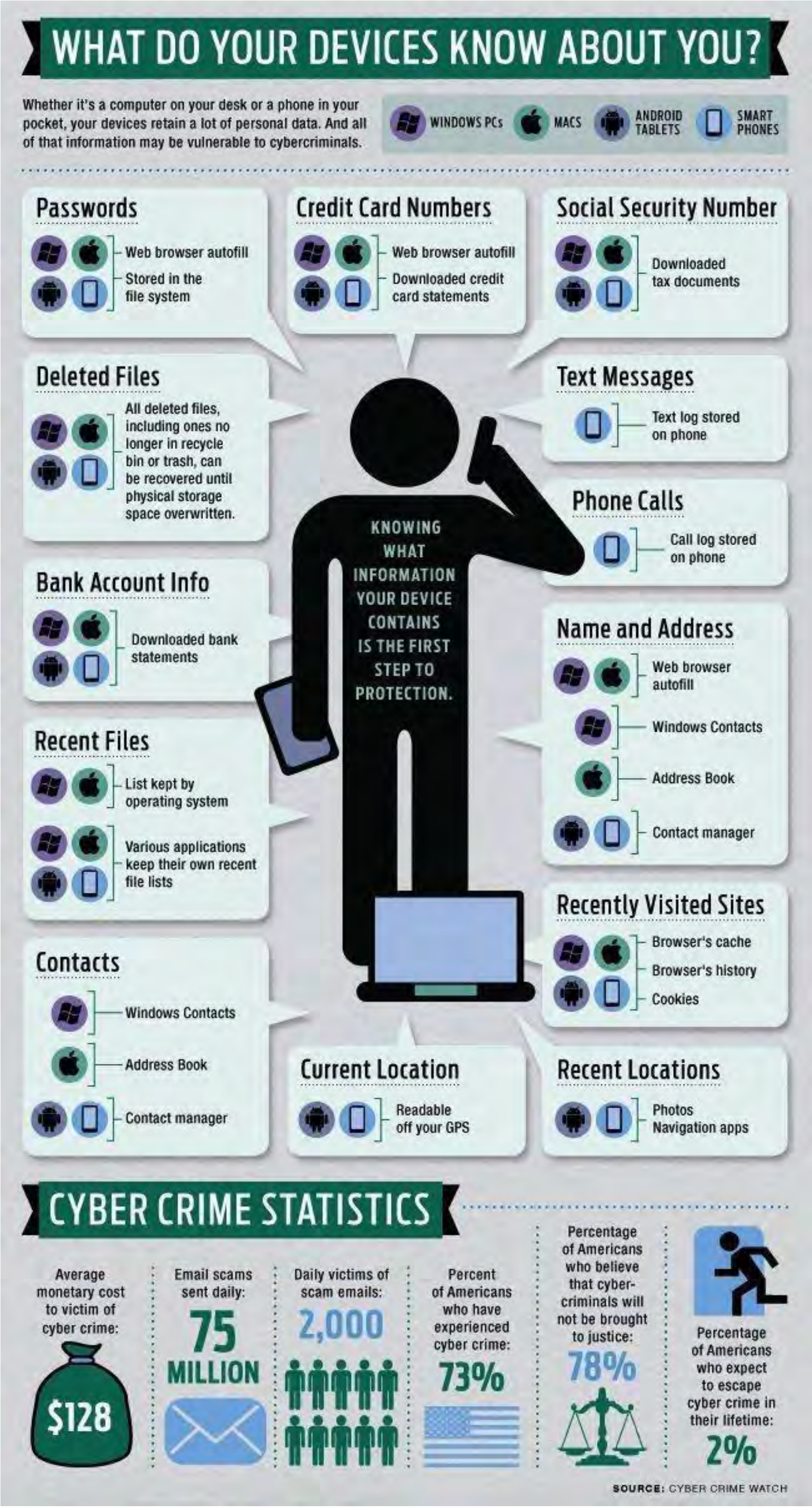
Updates to [redacted] may automatically add additional capabilities within each group. Learn more

Cancel

For example, if a child's toy that is IoT wants access to your contacts you should ask yourself why that would matter, and if you want to give that toy access. Many times, an App can still function with limited access to your different storage areas, and other Apps on your smart device.

Personas

When dealing with IoT devices it is important to take a step back and decide with this convenience what am I willing to sacrifice. To limit what you sacrifice I have employed the use of personas. For each segmentation of the device, I have a different persona that allows me to protect that area of my life. When setting up an Amazon Alexa device I set up under an alternative name, such as Jane Doe. I set up the preference that I might have for the device, but have the email address not be the primary one setup with my Amazon account. Although the convenience of the Amazon Alexa for shopping is there, I have selected to not have my persona share those personal details. I have the coordinating Apps for Alexa to have different personas as well such as my Spotify account. As each of the personas come together in that central device the image of who I am and the data I am sharing is blurred to the digital AI. The minor sacrifice to certain features is worth it for the privacy of my overall actual data.



WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

WINDOWS PCs · MACS · ANDROID TABLETS · SMART PHONES

Passwords
- Web browser autofill
- Stored in the file system

Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

Social Security Number
- Downloaded tax documents

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
- Text log stored on phone

Phone Calls
- Call log stored on phone

Bank Account Info
- Downloaded bank statements

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Recent Files
- List kept by operating system
- Various applications keep their own recent file lists

Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

Contacts
- Windows Contacts
- Address Book
- Contact manager

Current Location
- Readable off your GPS

Recent Locations
- Photos
- Navigation apps

KNOWING WHAT INFORMATION YOUR DEVICE CONTAINS IS THE FIRST STEP TO PROTECTION.

CYBER CRIME STATISTICS

- Average monetary cost to victim of cyber crime: $128
- Email scams sent daily: 75 MILLION
- Daily victims of scam emails: 2,000
- Percent of Americans who have experienced cyber crime: 73%
- Percentage of Americans who believe that cyber-criminals will not be brought to justice: 78%
- Percentage of Americans who expect to escape cyber crime in their lifetime: 2%

SOURCE: CYBER CRIME WATCH

What are the privacy controls?

When you take the perspective of how much data your devices know about you it is important to start adjusting to your life of how to deal with the control of these devices and their data. The following illustration is the perfect example of how much data gets stored in the systems that you access.

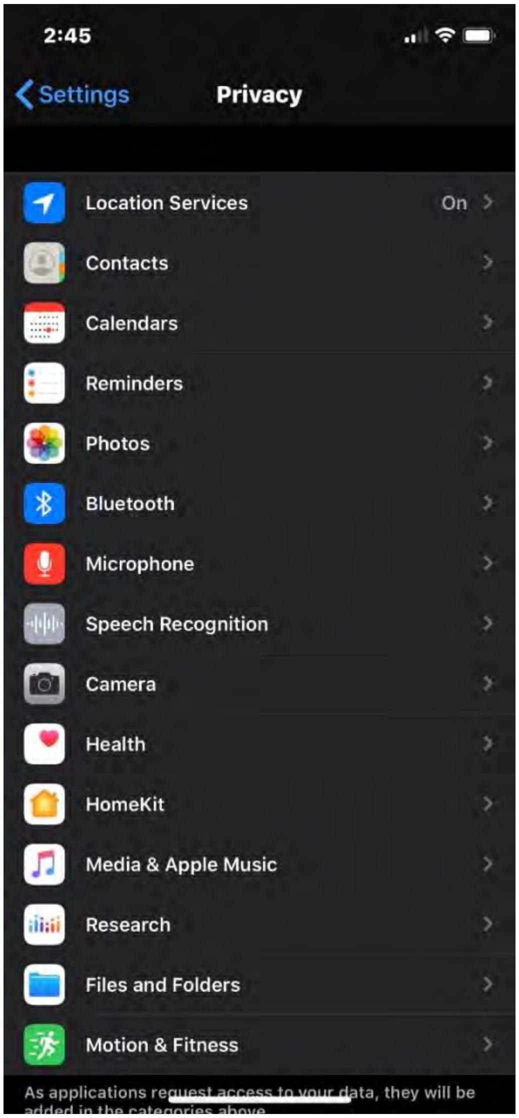
[12]

Smartphones

As the integrating hub to most of your information, it is important to take time and regularly clear some of the data that has leaked onto this device. Many individuals use third-party applications or cleaners that are designed to clear this data. However, in doing so you are granting a large level of access to your device to these third-party programs. It is always important when evaluating an App that you look at who the manufacturer is of that App and do your due diligence on the company and what level of rights and permissions they are accessing. Alternatively, are functions built into your device that allow you to clean permissions and data fragments with the native firmware of the device. Although they might not get as detailed, it is all done through access controls built into your device.

[12] (http://symbianone.com/2018/02/infographic-devices-know/)

Apple



2:45

Settings Privacy

Location Services On

Contacts

Calendars

Reminders

Photos

Bluetooth

Microphone

Speech Recognition

Camera

Health

HomeKit

Media & Apple Music

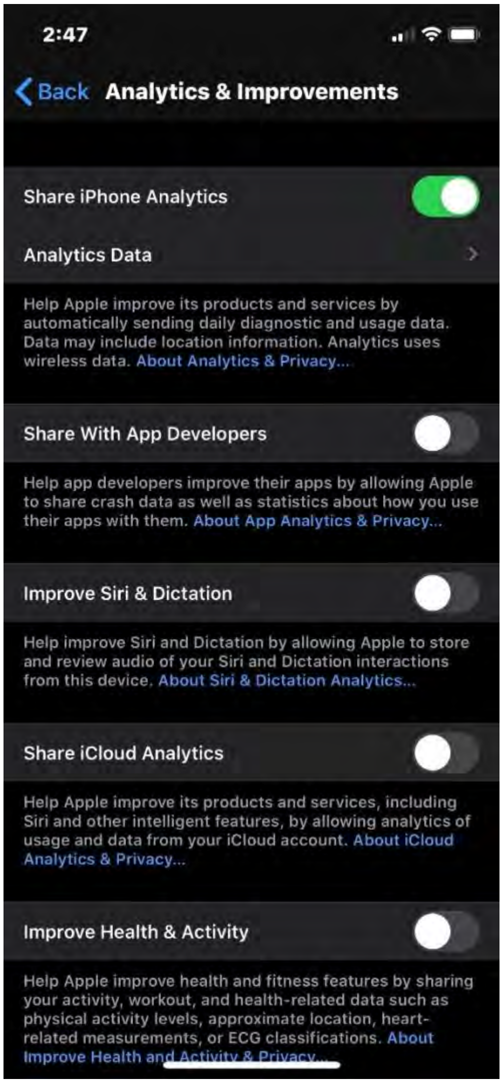
Research

Files and Folders

Motion & Fitness

As applications request access to your data, they will be added in the categories above.

Apple has publicly come out over the last few years siding with the side of privacy over that of government access. However, the perspective on that privacy is very different when you take it with the perspective of your family in mind. First, you can go to the Privacy section of your device and review the individual controls for each of the different Apps and their access. Many will allow for adjustments and restrictions to be made. The exceptions to that are with some of the many default Apps offered by Apple.



2:47

Back Analytics & Improvements

Share iPhone Analytics: On

Analytics Data

Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information. Analytics uses wireless data. About Analytics & Privacy...

Share With App Developers: Off

Help app developers improve their apps by allowing Apple to share crash data as well as statistics about how you use their apps with them. About App Analytics & Privacy...

Improve Siri & Dictation: Off

Help improve Siri and Dictation by allowing Apple to store and review audio of your Siri and Dictation interactions from this device. About Siri & Dictation Analytics...

Share iCloud Analytics: Off

Help Apple improve its products and services, including Siri and other intelligent features, by allowing analytics of usage and data from your iCloud account. About iCloud Analytics & Privacy...

Improve Health & Activity: Off

Help Apple improve health and fitness features by sharing your activity, workout, and health-related data such as physical activity levels, approximate location, heart-related measurements, or ECG classifications. About Improve Health and Activity & Privacy...

Important details in the data-sharing agreements that can allow you data to go back to Apple and its associated vendors which can include all the App manufacturers. These functions that are down in the menu options are not required for your device to function and minimizing as many of them as possible will allow you to maintain the best possible protection for your data.

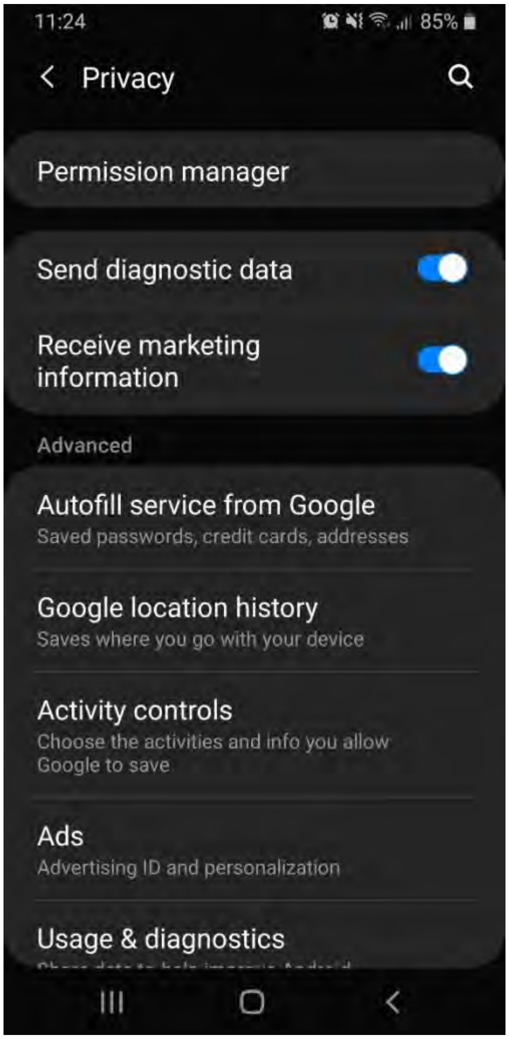
Apple Family Sharing

With smartphones becoming family-focused and wanting to provide options for family management it is important to be aware of how these functions work to protect your family data.

With Apple devices, the “Family Sharing” feature has been designed for iPhone 8 and above users. When this is active it allows the family to be managed by an admin user. This is a great option to keep track of your devices with your children, etc. There are great values to the ability to monitor data on the different devices with quick checks of browsing history and controlling purchases. However, it is important to note that this also allows the data to be seen across different devices. The biggest concern is with the location data tracking that is available between the devices. As mentioned, this is the most common data leak from smartphones that puts you at risk. Be mindful of the selection or enabling of this function as if one device in the family is compromised, they all are.

Android

Android is a more generalized system with each manufacturer doing a different spin on it. Typically, you will still see the privacy options and controls that can be adjusted.



11:24 85%

Privacy

Permission manager

Send diagnostic data ●

Receive marketing information ●

Advanced

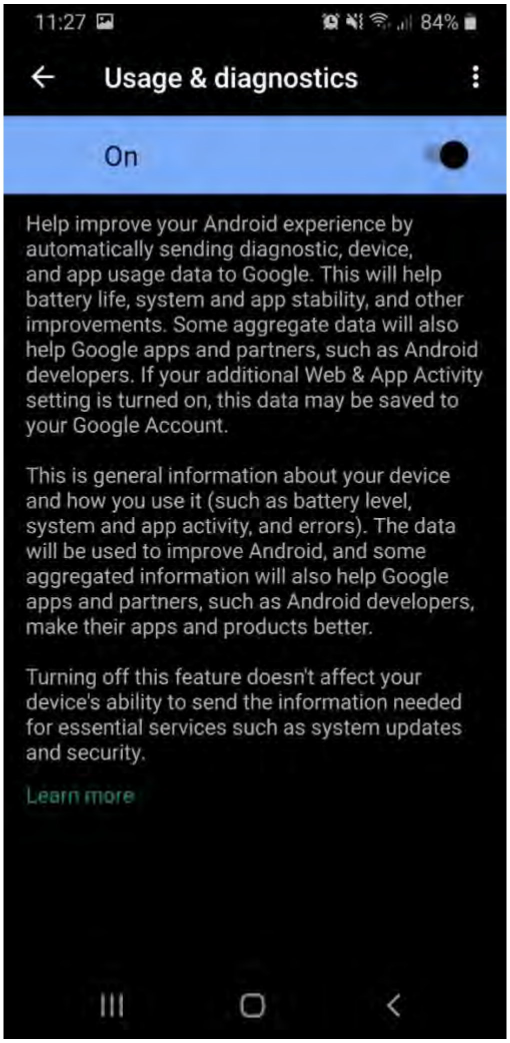
Autofill service from Google
Saved passwords, credit cards, addresses

Google location history
Saves where you go with your device

Activity controls
Choose the activities and info you allow Google to save

Ads
Advertising ID and personalization

Usage & diagnostics



11:27 84%

Usage & diagnostics

On ●

Help improve your Android experience by automatically sending diagnostic, device, and app usage data to Google. This will help battery life, system and app stability, and other improvements. Some aggregate data will also help Google apps and partners, such as Android developers. If your additional Web & App Activity setting is turned on, this data may be saved to your Google Account.

This is general information about your device and how you use it (such as battery level, system and app activity, and errors). The data will be used to improve Android, and some aggregated information will also help Google apps and partners, such as Android developers, make their apps and products better.

Turning off this feature doesn't affect your device's ability to send the information needed for essential services such as system updates and security.

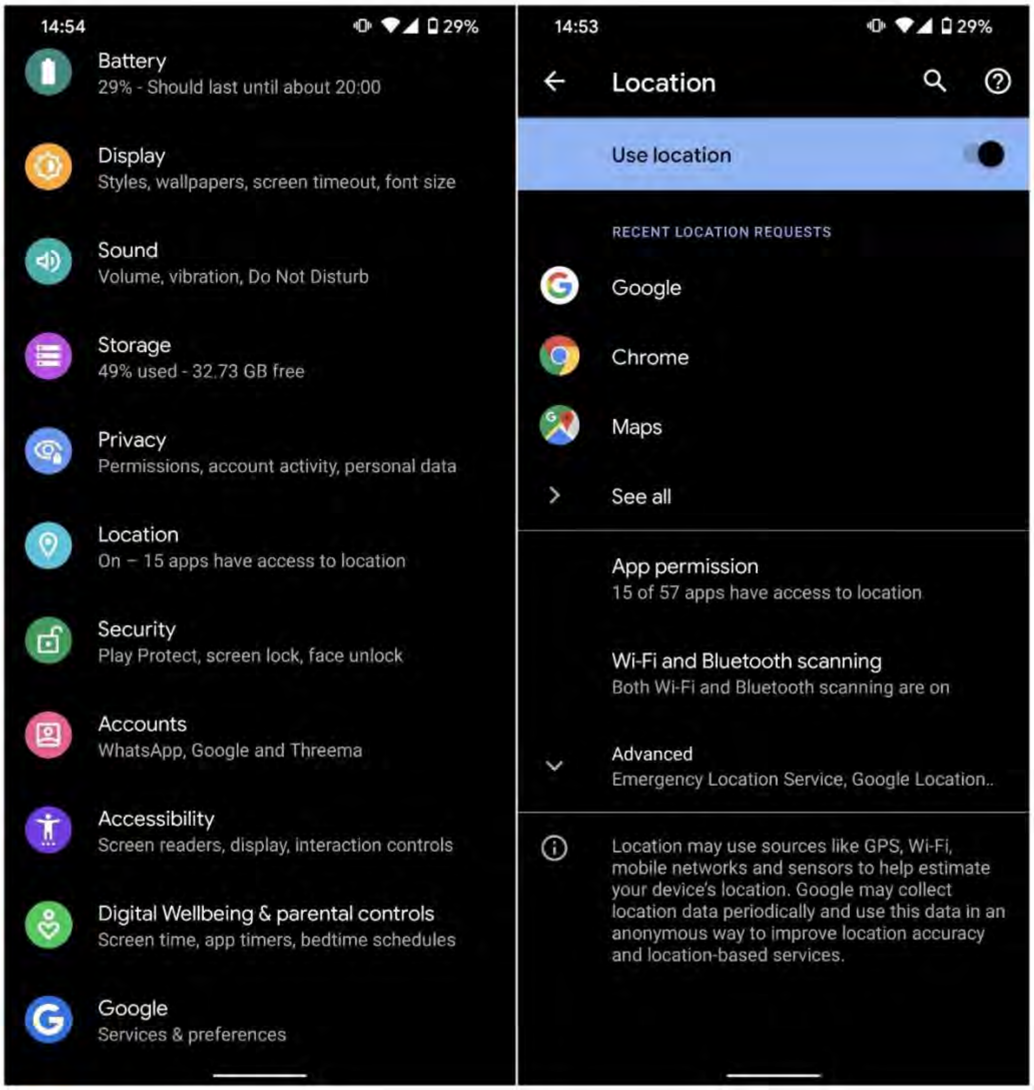
Learn more

Turn off options such as send diagnostic data, or receive marketing materials and you have already started to share less data about yourself and how you are using your device. Other options to be mindful of are Autofill options that are linked to your email accounts.

Finally, review the Usage and diagnostics settings to ensure that you are turning those off. This will not affect the usage of the device just the data you are choosing to share back to the manufacturer and all the other App developers out there.

Location Services

One of the most common passive data leaks from a device can come from location services. Pay attention to your device and which of the many Apps have access to this feature. When an App has access it can activate location services even when you thought the service was off. This is an important feature that you want to be able to pick and choose when your physical location is being recorded.



14:54 29%

Battery
29% - Should last until about 20:00

Display
Styles, wallpapers, screen timeout, font size

Sound
Volume, vibration, Do Not Disturb

Storage
49% used - 32.73 GB free

Privacy
Permissions, account activity, personal data

Location
On – 15 apps have access to location

Security
Play Protect, screen lock, face unlock

Accounts
WhatsApp, Google and Threema

Accessibility
Screen readers, display, interaction controls

Digital Wellbeing & parental controls
Screen time, app timers, bedtime schedules

Google
Services & preferences

14:53 29%

Location

Use location ●

RECENT LOCATION REQUESTS

Google

Chrome

Maps

See all

App permission
15 of 57 apps have access to location

Wi-Fi and Bluetooth scanning
Both Wi-Fi and Bluetooth scanning are on

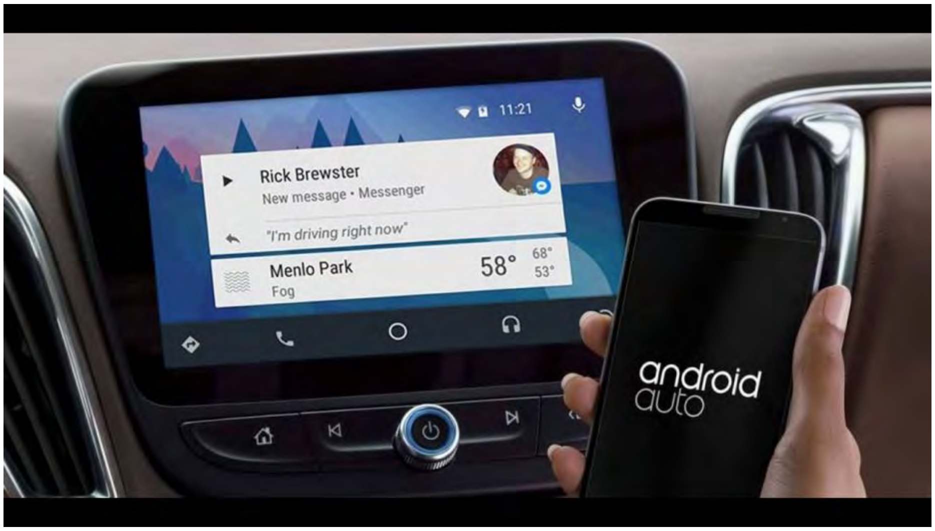
Advanced
Emergency Location Service, Google Location..

Location may use sources like GPS, Wi-Fi, mobile networks and sensors to help estimate your device's location. Google may collect location data periodically and use this data in an anonymous way to improve location accuracy and location-based services.

The screenshot from an Android device shows you which of the many Apps has access to the location function in the settings of the device. The same settings exist on Apple devices as well. Make sure you want to allow this access on each and every one of the Apps. Check back to this area often as Apps will update and have new features that will want access to this popular feature in smartphones.

Car Connections

When traveling with your smartphone it is important to keep in mind the connections your devices are making. Just like shaking the hand of every person your meet might cause you to become ill the same can happen with your smart device and the data you share. The perfect example of this is the use of rental cars. As you plugin to charge your device to a rental car you are often asked if you want to connect to the cars system.



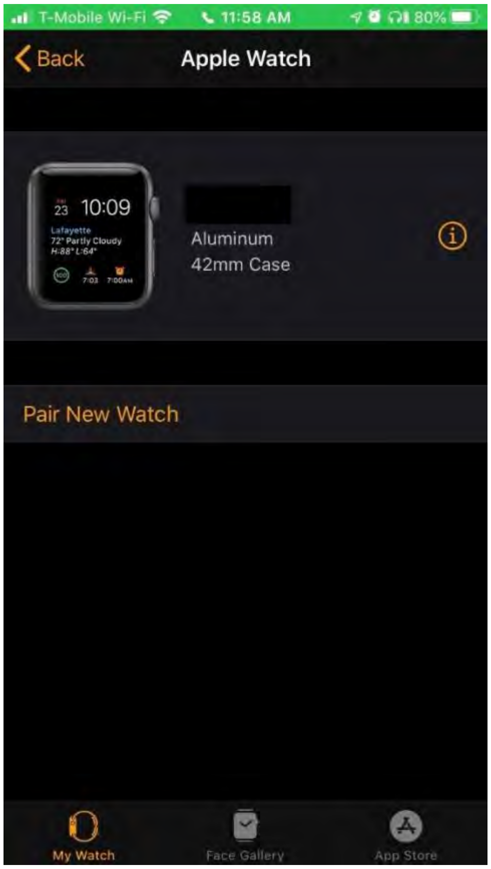
That connection at the time might be convenient, but the long-term data sharing is not. Fragments and details of your synchronized device can be left behind in the vehicle and a trained advisory can capture this data and use it. When offered options for the connection it is important to only connect in a vehicle that you are in control of.

Once you select the connection know that your data will exist on this vehicle in some form or another. Protect your activities that you do and what you access while connected to reduce the spread of your information.

Smartwatches & Fitness Bands

When working with a smartwatch it is important to remember that copies of your data exist on the smartwatch independent of your primary device. The best means for controlling the data between the two devices is to manage data synchronization.

With devices such as the Apple Watch once the device is paired there is a constant synchronization occurring. Keep in mind this synchronization is controlled with the Bluetooth connection. If you drop the Bluetooth connection the watch will continue to function but not share data. This might change based on the model of the watch. If the Apple Watch has cellular connection even the loss of Bluetooth connection will not stop the synchronization. Choose your model based on the controls you wish to put in place.



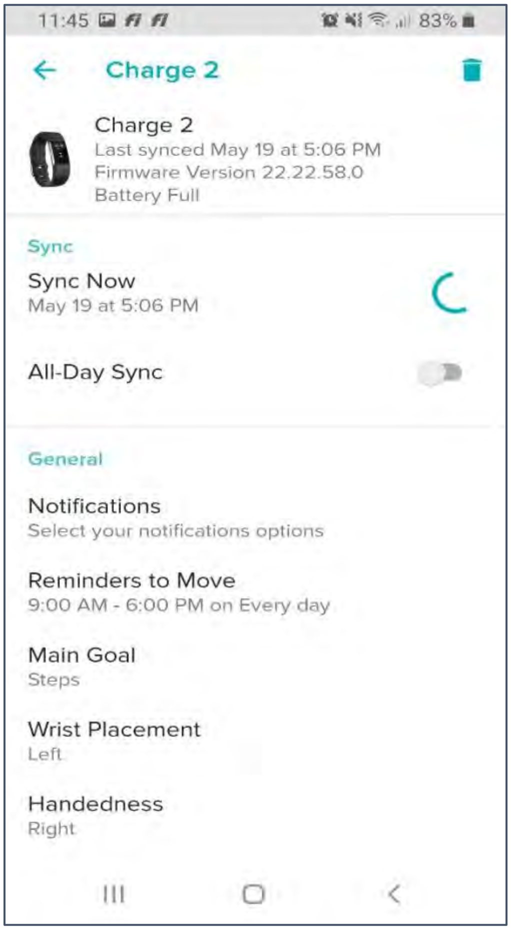
T-Mobile Wi-Fi 11:58 AM 80%

Back Apple Watch

23 10:09
Lafayette
72° Partly Cloudy
H:88° L:64°
7:03 7:00AM

[redacted]
Aluminum
42mm Case

Pair New Watch



11:45 83%

Charge 2

Charge 2
Last synced May 19 at 5:06 PM
Firmware Version 22.22.58.0
Battery Full

Sync

Sync Now
May 19 at 5:06 PM

All-Day Sync

General

Notifications
Select your notifications options

Reminders to Move
9:00 AM - 6:00 PM on Every day

Main Goal
Steps

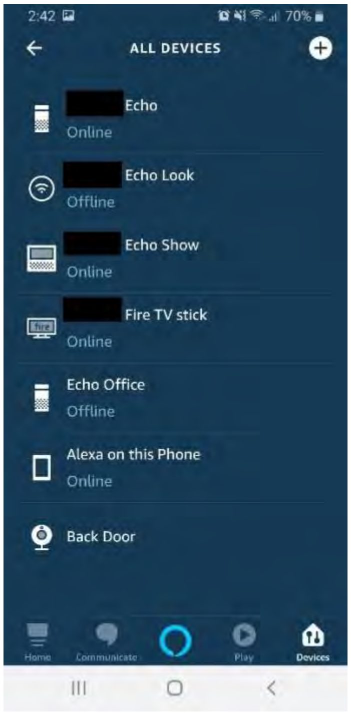
Wrist Placement
Left

Handedness
Right

When you select times for synchronization you can limit the data that is on the secondary device. If you desire to have your data synchronize constantly it is important to keep in mind the signal that you are leaving open between the two devices. Bluetooth is the most common method of ongoing synchronization and walking around with your Bluetooth broadcasting is not advised.

All the data is still shared, but by controlling the signal time you can control when you might be the highest risk for issues.

Home Assistants



2:42 70%

ALL DEVICES

[redacted] Echo
Online

[redacted] Echo Look
Offline

[redacted] Echo Show
Online

[redacted] Fire TV stick
Online

Echo Office
Offline

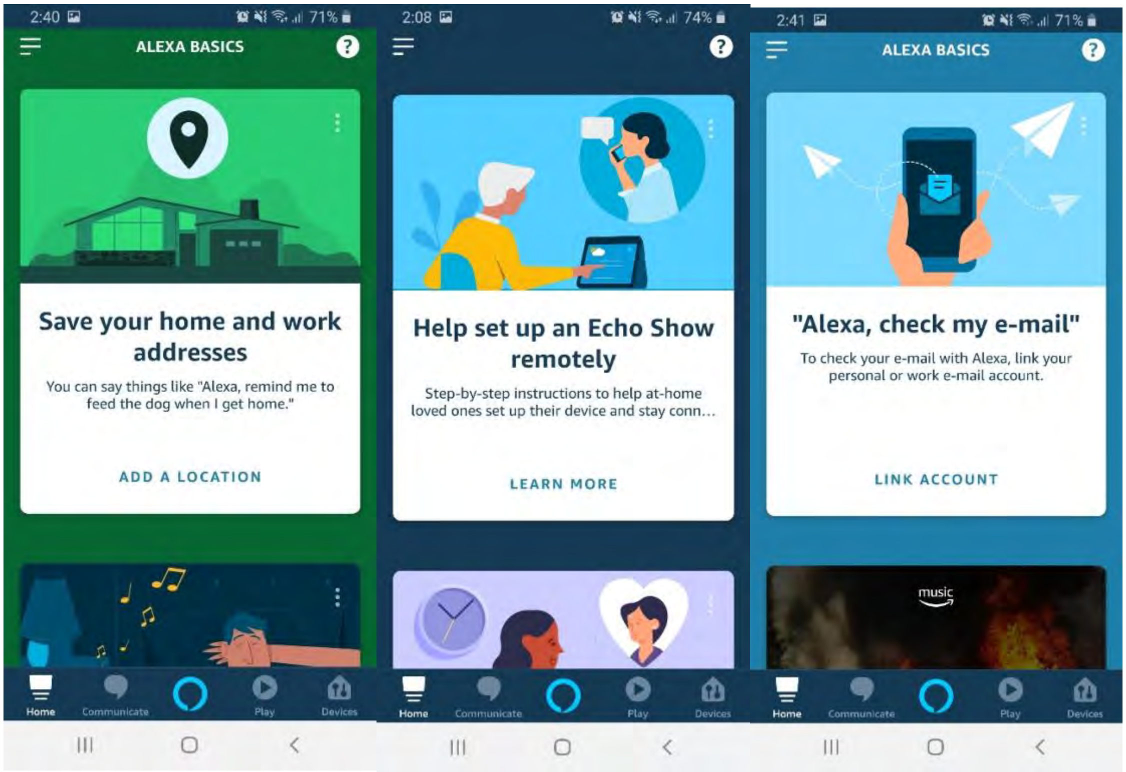
Alexa on this Phone
Online

Back Door

The friendly voice reading your news in the morning to you from you Google Home or Amazon Echo might be listening to more than you expected. With these AI growing in popularity it is important to limit your exposure to the data you share. While practicing personas and sub networking you can also adjust privacy controls on the device to make sure you can still have the convenient help in the kitchen while keeping your data.

Remember that you need to make sure you check the settings for each of the devices you have. Some of the devices might surprise you that are controlled through the App. Examples such as smart TV attachments and even your phone might show up.

When looking at the Amazon Alexa style device it is important first to remember to listen to what they ask before you just say yes. Lately, the Alexa device has learned voices and wants to identify you with your voice. When you use the App, you will see all the different options that they want to control, remember it is important to review them all and make the smart decision when it comes to your data. There is no need to use all the features remember everything is optional.



2:40 71%

ALEXA BASICS

Save your home and work addresses

You can say things like "Alexa, remind me to feed the dog when I get home."

ADD A LOCATION

2:08 74%

Help set up an Echo Show remotely

Step-by-step instructions to help at-home loved ones set up their device and stay conn...

LEARN MORE

2:41 71%

ALEXA BASICS

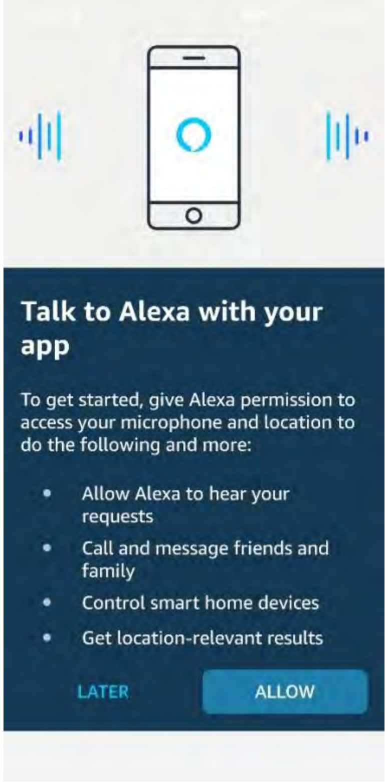
"Alexa, check my e-mail"

To check your e-mail with Alexa, link your personal or work e-mail account.

LINK ACCOUNT

Make sure you maintain your persona with your voice or simply decline to be identified by your voice. All AI devices similar to this must ask for permission before gaining access so pay attention.

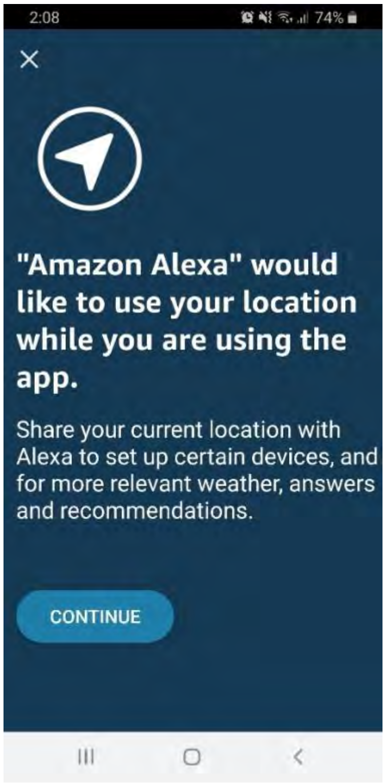
Also, many controls can be accessed through the App interface on your smart device that is controlling the device.



Talk to Alexa with your app

To get started, give Alexa permission to access your microphone and location to do the following and more:

- Allow Alexa to hear your requests
- Call and message friends and family
- Control smart home devices
- Get location-relevant results



"Amazon Alexa" would like to use your location while you are using the app.

Share your current location with Alexa to set up certain devices, and for more relevant weather, answers and recommendations.

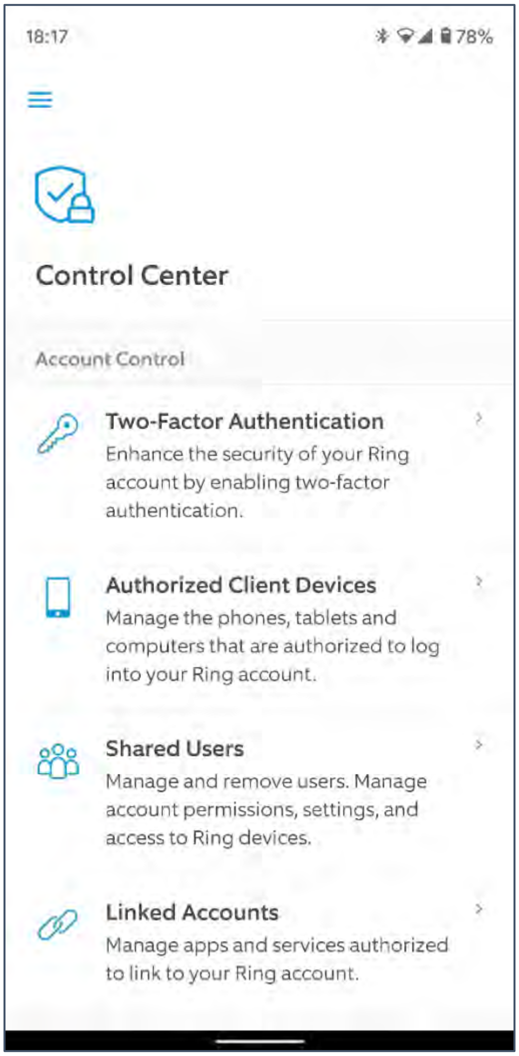
In the end, there is a convenience to the smart home assistant, but balance that convenience with the data you choose to share in the process with minor adjustments to the different App controls.

Home Security

When looking at the overall security options for a home the possibilities are endless in the world of IoT. Setting up each of those systems to maximize your privacy and security can come down to a few key factors.

Two-Factor Authentication

This extra layer of security allows you to help stop unauthorized parties from access your information. With many devices such as the Ring Doorbell, you can enable this option.



18:17 78%

Control Center

Account Control

Two-Factor Authentication
Enhance the security of your Ring account by enabling two-factor authentication.

Authorized Client Devices
Manage the phones, tablets and computers that are authorized to log into your Ring account.

Shared Users
Manage and remove users. Manage account permissions, settings, and access to Ring devices.

Linked Accounts
Manage apps and services authorized to link to your Ring account.

Stop Sharing

With many of the security additions in IoT, it allows you to work and share data with other similar devices in an area. This is never a good idea and you should always keep your data to yourself. Do not allow the sharing of information from one security system to your neighbors to create a digital neighborhood watch. Remember at the end of the day you do not know how your neighbors configured their devices and you sharing with them opens you up to all the mistakes they might have made.

Keep your Login Private

Even with multiple people in a home, it is important with the security systems to keep the login to these systems private. Do not share the App control with many people in a home keep it limited to the two primary adults.

Storage Details

With many of the IoT security systems keep in mind there are subscription plans and storage of data. The data for a subscription plan is typically not stored on your local smart device and is stored with the provider of the service. When this is the case it is important to understand how you can access the data and the data retention policy associated with your data. Just because you have deleted your data in the system doesn't mean it is gone. Typically, the data will move from the active state in your account to a pending state where it waits out the data retention period.

Children's Devices

The toys of today are growing smarter and smarter. There is a large variety of different devices that can be used by children that are connected and considered IoT. In this section, we are going to focus on more of the stand-alone systems. Systems such as gaming devices should be watched as well as they are also a connected computer with a variety of capabilities.

The primary goal of an IoT toy is the connection and affirmation it can provide to a child. So, when limiting and protecting yourself and your family from these types of devices it is all about the control of the data.

What types of data are collected?

When dealing with IoT devices that are for an emotional bond and affirmation most of the devices go through a collection stage with the setup of the device. In this collection stage, it is important for parents to actively participate to understand what your child might be sharing with the device. Many times, the questions are general, but they can be targeted and are recorded for reference by the device.

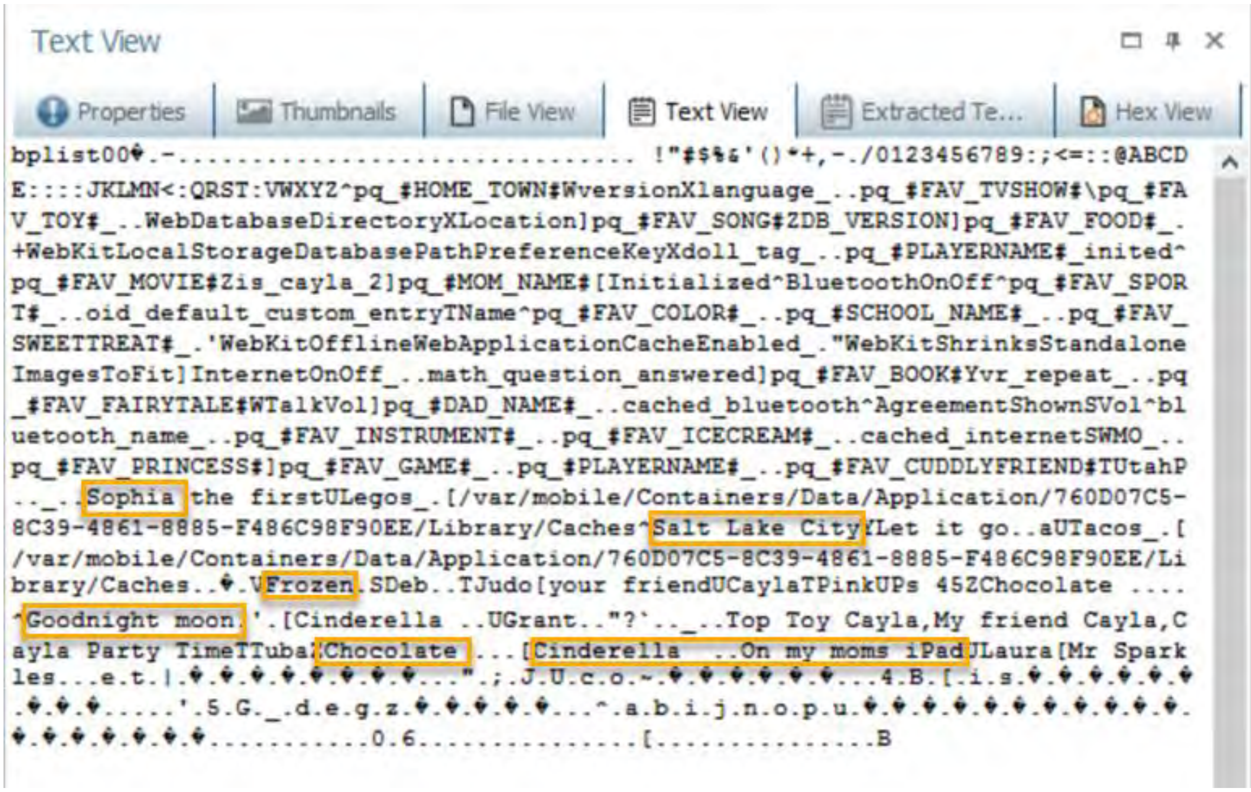
An example can be found with the Cayla Doll.

The following is from the Cayla website:

"My Friend Cayla is like a real friend, she's so much more than a talking doll or app toy! Get to know her by asking questions about her family, favorite foods, hobbies, pets, and more. Cayla also loves to answer tricky questions about things like animals, countries, and famous people. She can also play games, tell stories, and talk about pictures in her photo albums. Cayla is 18" tall and comes with a hairbrush and mirror. Download the free app to an Android or iOS smart device and connect to Cayla via Bluetooth Wireless Technology. There are multiple safeguards in place to make her internet safe. Cayla can understand almost anything you say by using speech-to-text technology."

Cayla will ask for the name of the child, and the names of their parents. She will continue to ask questions such as where the child goes to school, favorite movies, etc. This is where doing the setup together makes a big difference to the base data recorded in the IoT device is what you want to share.

Here is an example of some of the data that was seen in the Cayla App after the setup was done.



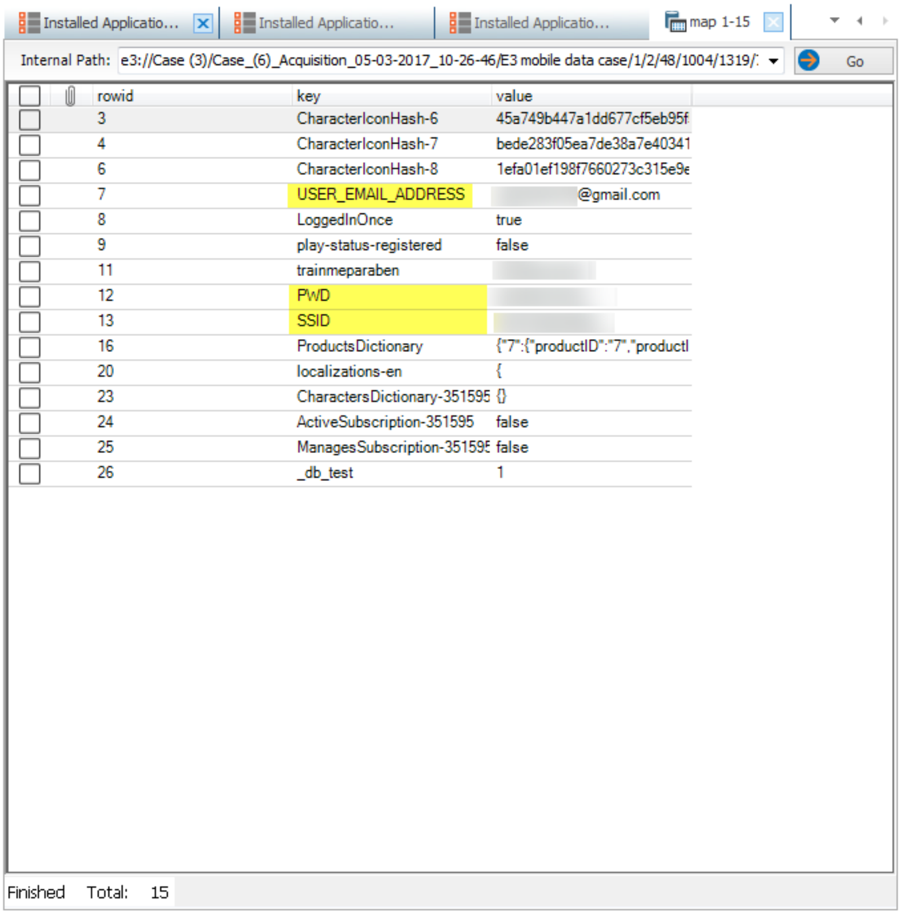
```
bplist00�.-................................ !"#$%&'()*+,-./0123456789:;<=::@ABCD
E::::JKLMN<:QRST:VWXYZ^pq_#HOME_TOWN#WversionXlanguage_..pq_#FAV_TVSHOW#\pq_#FA
V_TOY#_..WebDatabaseDirectoryXLocation]pq_#FAV_SONG#ZDB_VERSION]pq_#FAV_FOOD#_.
+WebKitLocalStorageDatabasePathPreferenceKeyXdoll_tag_..pq_#PLAYERNAME#_inited^
pq_#FAV_MOVIE#Zis_cayla_2]pq_#MOM_NAME#[Initialized^BluetoothOnOff^pq_#FAV_SPOR
T#_..oid_default_custom_entryTName^pq_#FAV_COLOR#_..pq_#SCHOOL_NAME#_..pq_#FAV_
SWEETTREAT#_.'WebKitOfflineWebApplicationCacheEnabled_."WebKitShrinksStandalone
ImagesToFit]InternetOnOff_..math_question_answered]pq_#FAV_BOOK#Yvr_repeat_..pq
_#FAV_FAIRYTALE#WTalkVol]pq_#DAD_NAME#_..cached_bluetooth^AgreementShownSVol^bl
uetooth_name_..pq_#FAV_INSTRUMENT#_..pq_#FAV_ICECREAM#_..cached_internetSWMO_..
pq_#FAV_PRINCESS#]pq_#FAV_GAME#_..pq_#PLAYERNAME#_..pq_#FAV_CUDDLYFRIEND#TUtahP
.._..Sophia the firstULegos_.[/var/mobile/Containers/Data/Application/760D07C5-
8C39-4861-8885-F486C98F90EE/Library/Caches^Salt Lake CityYLet it go..aUTacos_.[
/var/mobile/Containers/Data/Application/760D07C5-8C39-4861-8885-F486C98F90EE/Li
brary/Caches..�.VFrozen.SDeb..TJudo[your friendUCaylaTPinkUPs 45ZChocolate ....
^Goodnight moon.'.[Cinderella ..UGrant.."?`.._..Top Toy Cayla,My friend Cayla,C
ayla Party TimeTTuba:Chocolate ...[Cinderella  ..On my moms iPadULaura[Mr Spark
les...e.t.|.�.�.�.�.�.�.�.�...".;.J.U.c.o.~.�.�.�.�.�.�...4.B.[.i.s.�.�.�.�.�.�
.�.�.�.....'.5.G._.d.e.g.z.�.�.�.�.�...^.a.b.i.j.n.o.p.u.�.�.�.�.�.�.�.�.�.�.�.
�.�.�.�.�.�.�...........0.6................[...............B
```

The data highlighted was the bits of information that we shared in the setup that we saw again stored in plain text in the App. Although a normal person would not go through the trouble to find this data an average expert would be able to get these pieces of data and immediately know enough to lure a child into a conversation either in person or online.

I TALK, LISTEN & LEARN!
WE'LL NEVER RUN OUT OF FUN THINGS TO DO! (SERIOUSLY.)
Let's go on an adventure!
Fisher-Price
SMART TOY
3-8

Other toys such as the Fisher Price Bear can store data about what your child likes to do. This device is designed to identify play activities with the camera in its nose. It can even tell when your child hugs it with the accelerometer in the chest. The data that can come from devices like this are not always questions and answers, but items such as your network access details which can leave your home vulnerable to attackers.

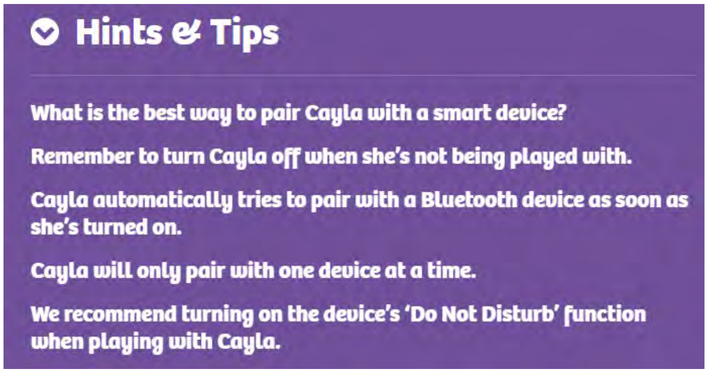
An example can be found below from the App associated with the bear.



Internal Path: e3://Case (3)/Case_(6)_Acquisition_05-03-2017_10-26-46/E3 mobile data case/1/2/48/1004/1319/:

rowid	key	value
3	CharacterIconHash-6	45a749b447a1dd677cf5eb95f
4	CharacterIconHash-7	bede283f05ea7de38a7e40341
6	CharacterIconHash-8	1efa01ef198f7660273c315e9e
7	USER_EMAIL_ADDRESS	[redacted]@gmail.com
8	LoggedInOnce	true
9	play-status-registered	false
11	trainmeparaben	[redacted]
12	PWD	[redacted]
13	SSID	[redacted]
16	ProductsDictionary	{"7":{"productID":"7","productI
20	localizations-en	{
23	CharactersDictionary-351595	{}
24	ActiveSubscription-351595	false
25	ManagesSubscription-35159£	false
26	_db_test	1

Finished Total: 15



Hints & Tips

What is the best way to pair Cayla with a smart device?

Remember to turn Cayla off when she's not being played with.

Cayla automatically tries to pair with a Bluetooth device as soon as she's turned on.

Cayla will only pair with one device at a time.

We recommend turning on the device's 'Do Not Disturb' function when playing with Cayla.

Don't forget that the toys have to connect to a device just like the other IoT devices. With that in mind be careful about the Bluetooth connection with the device you are pairing with. With child's toys, you can setup a dummy phone that is only to connect with these toys that is not your primary phone. This way you isolate the devices to the single non-primary device with no additional data on the device.

General Rules of IoT Devices

When you have an IoT device in your home it is a commitment to maintaining it, similar to a plant. You must keep it powered, and up to date with patches that might release from the manufacturers. One of the easiest ways to keep up on the trends associated with your device is to follow the manufacturer on social media.

Watch for hashtags that are associated with your particular device and feedback from other users. IoT is still a fairly new thing and people bring out flaws that they find and will tag the manufacturers to see if it is normal.

What can happen with a compromised device?

SAM Seamless Network has published a report on the IoT devices -- US households containing an average of 17 smart devices while EU homes have roughly 14 devices -- most likely to come under attack. TVs, kitchen appliances, and lighting are often targeted, but security cameras now make up 47% of vulnerable devices.[13]

After all of these changes to how you are using your devices, it is important to understand what can happen with a compromised device. There are risks online no matter what you are using and how you are connecting. Many of those same risks can come in via the path of your connected devices. Here are some of those risks broken down for a quick understanding.

Ransomware

Ransomware is a form of malware *that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.*[14]

Although this is uncommon to come in via the sector of connected devices it is important to note since you will be receiving emails from the device manufacturers once you set up an account. It is important to watch for the basics in the email structure to determine if it could be a phishing attack or not.

[13] Cybersecurity: These are the Internet of Things devices that are most targeted by hackers, Danny Palmer, June 12, 2019

[14] Ransomware explained: How it works and how to remove it, Josh Fruhlinger, December 19, 2018

1. **Who is it from?**

   Check the domain name and confirm it is from the actual manufacturer of your IoT device. If it is not or comes from an odd variation chances are it is a phishing attack trying to get you to click on a link.

2. **Content**

   Many times, the content is very abrupt and urgent telling you there is a security issue, etc. With an IoT device, it is important to note that many times security issues will be notified to you in the App, not in an email.

3. **Don't click**

   This is the only way ransomware can infect you is if you click on a link in the message. In general, just don't click. If you don't know the sender and you don't know the content then you don't need to click. Delete and move on.

Malware

Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems.[15]

You might be thinking that ransomware is also malware and in a lot of ways, it is as it had malicious intent on your system. Malware is the larger umbrella that covers a lot of code that is out for ill intent. When it comes to IoT devices the issue with malware has not been as large as you might think. The most common devices that end up hacked and potentially infected with malware are cameras. Many times, they broadcast an open IP address out that allows hackers to hijack the device and introduce themselves and malware into your network. These types of flaws are with the manufacturer and often when they are found they are patched.

From previous recommendations running the IoT devices on a separate subnet will help with this issue, but you are still at risk. *Many IoT devices have been known to have vulnerabilities that allow attackers to remotely access or control them from the internet, while some have been found to have weak passwords that cannot be changed. In the worst-case scenario, devices will be found to have both.*[16] This brings us back to the basics mentioned earlier about picking good secure passwords and separating your persona based on the devices you are using. Nothing in the world of connected devices is 100% secure.

[15] (https://www.malwarebytes.com/malware/)

[16] (https://www.zdnet.com/article/iot-security-why-it-will-get-worse-before-it-gets-better/)

Spyware

Spyware is a broad category of malware designed to secretly observe activity on a device and send those observations to a snooper. That data can be used to track your activity online and that information can be sold to marketers. Spyware can also be used to steal personal information, such as account passwords and credit card numbers, which can result in identity theft and fraud.[17]

Spyware is another form of malware as they all stem from malicious software. The largest problem with spyware is that when you starting using IoT devices you typically start using more than one. The IoT devices all connect and into one network so a domino effect can take place so that once one device is compromised, they all are. The tactics are similar as discussed with ransomware where phishing attacks will be used.

The other side of spyware is to determine who might be interested in spying on you. If there is anyone that would be interested in watching you or your family on a camera if thieves might be interested in gaining access to be able to do a break-in. Finally, keep in mind in situations where family members might split off that access should be changed immediately after one of the parties has left the home to ensure that any potentially spying cannot take place.

What are the best practices?

In the end, it is all about being able to live with the technology in our lives without the risk of our lives from the technology. When dealing with anything that has access to as much data, images, location, and potentially personal information we go back to our best practices to make sure that we are as safe as possible.

First with any devices that are set up remember that you should never leave the settings at the default options. This is the easiest way for anyone to gain access to your devices and data. Follow the recommended best practices from earlier about the use of passphrases or long passwords done through a password generator. If you are concerned about remembering the longer passwords use a password manager that has been tested and follows practices such as two-factor authentication to ensure that your keys are safe. Do not keep passwords in documents, spreadsheets, etc. They are not encrypted and are not secure for keeping your keys. Treat passwords just like the keys to your home, and don't just leave them lying around where anyone can gain access.

Second keep IoT devices on a separate network so that you can segment the data and the risk. Just like keeping your backyard secure for your dog or kids with a fence a segmented network allows the same thing with IoT devices being kept separate than the primary computers, and access to your network.

[17] Spyware In The IoT – This Year's Biggest Security Threat, Sam Bocetta, April 29, 2019

Next, keep your devices up to date. Following your providers in social media to keep track of trends will help you stay on the top of the curve for risks that might come from having devices. Make sure you are updating your Apps that control your devices regularly and manually checking for updates in addition to the automated updates. Make it part of your routine as it is just like keeping a plant alive with regular sunshine and water you need the latest patches and updates.

Finally start a digital “spring cleaning” with resetting your passwords, and networks at regular intervals. In my home, we reset our networks every six months to ensure that nothing could have leaked out or been at risk. These simple processes in your network will keep you ahead of the average attacker and keep you fresh with your security standards.

Information Exposed ™
June 2020 >> Version 1.0

Opt Out Online: Finding & removing personally identifiable information found on the Internet.™
June 2020 >> Version 10.0

World of Connected Devices Solved: Unerstanding the risks of smartphones and IoT devices.™
June 2020 >> Version 1.0

Hg HetheringtonGroup

paraben® corporation paraben.com