CONSUMER PRIVACY & IDENTITY QUARTERLY

VOL N°1 ISSUE N°1

DISCLAIMER

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

FOR MORE INFORMATION OR QUESTIONS EMAIL osd.ncr.osd.mbx.dodsmartcards@mail.mil

IN THIS ISSUE:

THE ROAD OF LIFE:
HOW YOUR ONLINE IDENTITY CHANGES THROUGH YOUR LIFE

From social media to forums, filled out surveys, online retail accounts, and beyond, your online identity takes shape from a wide variety of sources. Learn about these individual pieces that, when combined, form your online identity.

THE WORKING YEARS:
HOW TO KEEP YOUR IDENTITY SECURE THROUGHOUT YOUR WORKING LIFETIME

Working adults have a digital footprint spanning roughly 43 years, from the typical college graduation age (22) to the common retirement age (65). Learn about the biggest threats to your identity throughout your working years.

ALSO INSIDE:

FROM THE WOMB TO PRETEEN:
PROTECTING CHILDREN'S ONLINE IDENTITY BEFORE IT'S TOO LATE

THE TEENAGE YEARS:
KEEPING IDENTITIES SAFE WHILE TRANSITIONING TO ADULTHOOD

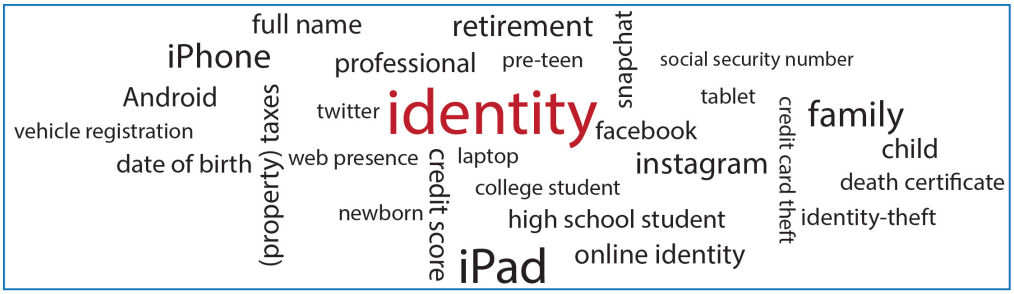
THE COLLEGE YEARS:
INDEPENDENCE LEADS TO NEW THREATS

RETIRE AWARE:
HOW TO PROTECT YOUR IDENTITY AFTER RETIREMENT

THE ROAD OF LIFE: HOW YOUR ONLINE IDENTITY CHANGES THROUGH YOUR YOUR LIFE'S JOURNEY

Who are you? It is an existential question that has been pondered since ancient times. The answer to that question is constantly changing. It is the key to understanding, navigating, and protecting your identity in an increasingly digital world.

With the Internet, social media, and massive data analytics employed by corporations and governments, your identity is no longer just who you are. It is what you do, what you say, what you watch, what you read, what you buy, what you look like, where you go, and with whom you associate. Online and offline identities have blended in ways that are persistent, traceable, and permanent. That expanding digital footprint is also under constant attack.



As the digital nature of identity continues to evolve, new threats have emerged. Sophisticated identity theft rings have been uncovered across the United States, costing consumers billions of dollars every year. Seemingly small information thefts can have international repercussions. Nefarious groups use social engineering and phishing schemes to trick individuals into divulging confidential information, thereby granting hackers access to secure networks.

These threats require strong countermeasures to guard against abuse and keep people safe. Governments and businesses must ensure sensitive records are encrypted and deploy advanced network traffic analytics to stop data breaches. Individuals must use strong unique passwords for online accounts and electronic devices, properly dispose of sensitive records, and monitor accounts for fraudulent activity.

The stakes could not be higher:

- Nearly 18 million Americans ages 16 and older were victims of identity theft in 2014, up from 12 million in 2008, according to the Bureau of Justice Statistics. Millions of young children were also victims.
- More than half of identity thefts are digital, according to the Center for Identity at University of Texas, Austin. The shift of identity into cyberspace gives thieves easier access to an almost unlimited pool of personally identifiable information (PII).
- The scale of attacks is growing. In 2015, health insurer Anthem Inc. reported that hackers stole 79 million individuals' PII, including names, Social Security numbers (SSN), addresses, employers, and income data. That same year, attackers also infiltrated the US Office of Personnel Management, stealing the SSNs and other sensitive data of 22 million people.
- Identity abuse increasingly enables dangerous activity. Millions of stolen credit card numbers and SSNs are powering illicit transactions on the Dark Web, terrorists routinely steal identities to facilitate travel and enter target countries, and there are ongoing attempts by terrorist groups to compromise the identities of United States military personnel on social media.

This issue of the Consumer Privacy & Identity Quarterly takes a "cradle to grave" look at identity, how it changes over the course of one's lifetime, and how technology, including biometrics and mobile devices, are making an impact. Writers delve into the primary online and offline identity attributes for young children, teens, college-age adults, working adults, retirees, and the deceased. Each article explores facets of identity, identifies risks to PII, and highlights safety measures for each age range. Together, the stories form a comprehensive map of identity and provide the best steps individuals can take to reduce their likelihood of becoming victims.

Controlling and monitoring what you do online, however, is just one component. Your family, friends, co-workers, and associates may post a great deal of information about you online. Throughout this magazine you will learn strategies to limit the amount of PII others can post or link to your identity.

To get more information on safeguarding PII, electronic devices, and online accounts pick up the newest version of the DoD Smart Book and Smart Cards by emailing osd.ncr.osd.mbx.dodsmartcards@mail.mil.

FORMATIVE FOOTPRINTS

PRE-BIRTH TO PRE-TEEN

Ninety-two percent of children in the U.S. have an online presence by the age of 2. Their digital footprints contain personally identifiable information that makes them prime targets for identity theft. Follow along to view the data available by age.

PRE-BIRTH

The digital footprint for children can begin before they are born. Thirty-four percent of mothers upload sonogram images of their child onto the Internet.

HOW VULNERABLE ARE CHILDRENS' IDENTITIES?

11% of children have SSNs that were misused

1 in 40 are the odds of a child becoming an ID theft victim before turning 18

35X ID theft affects children 35 times more than adults

PRE-TEEN (10-12)

Tablets, smartphones, laptops, Social networking websites, Online video websites, instant messaging apps, Sports teams/newsletters, Online gaming, Debit cards/ online spending/app purchases

INFANT (0-2)

Birth certificate, Social Security number (SSN), Baby Photos, Hospital/ immunization records, Palm and foot prints, DNA tests, Daycare registration forms, Parent-created e-mail and social network accounts

CHILDHOOD (5-9)

Public school registration forms (gender, race, SSN, address, DOB), School data shared with state, federal and private entities Social groups (ex. Girl Scouts), Mobile devices, Email and social networking

INTERNET USAGE BY AGE 9

89% Active Users

11% No use

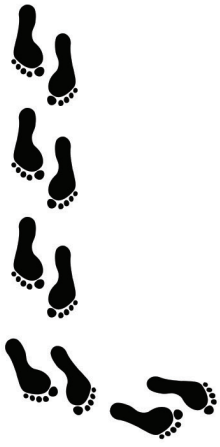
POPULAR SERVICES

Virtual world games **46%**

Email: **18%**

Facebook: **16%**

Instant Messaging: **9%**



PRESCHOOL (3-4)

Preschool registration forms (gender, date of birth (DOB), address,sibling names), Tablet computers/mobile games Online video (ex.Netflix for kids), Medical records

Sources: AVG, AllClearID, University of Texas at Austin Center for Identity

FROM THE WOMB TO PRETEEN: PROTECTING CHILDREN'S ONLINE IDENTITY BEFORE IT'S TOO LATE

Gone are the days of newborns sipping milk and napping peacefully without worrying about being hacked. Thanks to mobile devices and social media-savvy parents, many babies born in recent years have a burgeoning online presence that reaches back long before they could even say the word "Internet."

From photos shared online to posts gushing about a baby's cuteness, visible online presences exist for 92 percent of children in the United States by the age of two, according to a 2010 survey by AVG, an Internet security company. A third of American parents upload photos of newborns while six percent create email addresses and social network accounts for their children, according to the report.

Along with birth, hospital, school, and financial records, most parents do not realize the vast amount of their children's personally identifiable information (PII) that may be exposed online. That data, which could include Social Security numbers (SSN), dates of birth (DOB), and addresses, makes children a prime target for identity theft. The problem worsens as they age and share more about themselves online.

The risk factors vary for different age groups:

Pre-birth

The creation of digital identities for children can start months before birth with parents' posting ultrasound images online, often with PII, such as DOB, gender, and name. Baby shower registries may also release PII in places that are accessible online and indexed by search engines. Parents should review privacy policies before sharing information.

Infant (0 to 2)

After delivery, a child's first official records are created, including hospital reports, birth certificates, palm-prints and footprints, and DNA tests, if requested. These documents are confidential, but they are computerized. Children are not required to have a SSN, but most parents request them because they are necessary for claiming children as dependents on tax returns and requesting government services.

Because of a clean credit history, a child's unused SSN is valuable to identity thieves who can use it to file fraudulent tax returns, take out loans, or commit other crimes. According to a 2012 study by AllClearID, a company that provides identity protection services; one in ten children have had their SSNs misused, . Parents should regularly review children's credit reports and watch for unusual mail addressed to them.

Daycare services or nursery schools also gather and store PII, including DOB, gender, and address. The information is not easily accessed by outsiders, but these services vary in how they protect data and provide access to employees. Parents should ask about providers' record-keeping policies.

Some parents may create e-mail accounts, web domains, and social media profiles for children to reserve names on services and store communications, utilizing them as makeshift digital baby books. Information may be indexed by search engines and shared with advertisers for targeted advertisements and online tracking purposes. Again, parents should review the privacy policies of online services before using them.

Preschool (3 to 4)

Preschools often request DOB, medical information, emergency contacts, nationality, gender, and sibling names. Parents should understand how the information is stored and who has access.

Children in this age range usually make their first contact with computer games, typically on tablets and smartphones, and online video sources, such as Netflix. Some parents establish separate accounts for children on the services, which could create a digital record of their gaming and video preferences. Also, many free game apps contain third-party advertisements, including code that may allow tracking. If possible, parents should not use children's names for online services. Parents should also monitor apps and app stores, where children can install malicious

apps or make in-app purchases.

Public school (5 to 9)

Public schools require a large amount of PII, including SSN, race, and medical data. Most of the information is required, but some schools make providing a SSN optional. Immunization histories are requested for children, though parents can opt out for religious or medical reasons.

If parents request free or reduced price lunch, their financial information is collected and linked to the child's records. The risk to PII is enhanced in public schools because information is shared with state education authorities, the federal government, and third-party vendors, including standardized testing organizations. However, strict privacy laws govern dissemination of a child's PII.

A greater risk for school-age children is unsupervised access to the Internet. Studies show that children are using webmail and social networking services (SNS) at younger ages, thus placing photos and detailed information about themselves online. In a 2014 study, AVG found that of children aged six to nine, 89 percent were active online. About 18 percent used e-mail, 16 percent used Facebook (despite 13 being the minimum age to register an account), and nine percent used instant messaging, according to the study.

Joining extracurricular organizations can also establish digital records with PII. Group activities or member names and DOBs may be listed on their websites or electronic newsletters. Parents may be able to opt out of a group's online or media presence.

Pre-teen (10 to 12)

The risk of sharing PII through SNS increases as children gain more control of their online presence. Pre-teens often have unrestricted access to multiple devices at home, school, or the library. They also increase their use of SNS and instant messaging. Many children also share "check-ins," a record of visited places or real-time physical locations. Gaming is also a popular way for pre-teens to socialize online, sharing biographical information and chatting with other players. Parents should advise children about the danger of sharing too much information.

Some parents may give debit cards to their pre-teens. These cards can be used for online purchases, creating a record of spending habits. Parents should consider joint

accounts to easily monitor spending.

Along with other extracurricular activities, sports teams gather PII and records of athletes. Information about players and games may appear on their websites, newsletters, or local media outlets. However, many school and community teams provide forms that allow students to opt-out of having their name, picture, or other information published in directories. As a result, PII may still be published by outside media outlets; but, the school or team will be limited in the information they can provide.

By age 12, most children will have had an online presence for a decade. What is visible to the public depends on how much care they and their parents exercise.

THE TEENAGE YEARS: KEEPING IDENTITIES SAFE WHILE TRANSITIONING TO ADULTHOOD

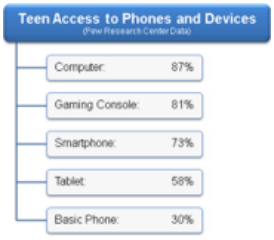
The teenage years are fraught with many changes and life transitions: biological, financial, and social. As the world becomes increasingly digital, teens increasingly face evolving digital threats and identity risks. These emerging digital aspects and expanding digital footprints can increase the difficulties faced by teens as they move through traditional identity milestones.

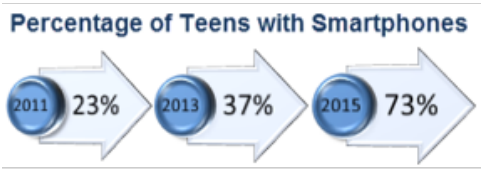
Expanding the Teenage Digital Footprint

Technology and the Internet have a rapidly expanding reach into the daily lives of teenagers. According to 2015 Pew Research Center data, 92 percent of teenagers accessed the Internet at least daily.

Teenagers are increasingly using smartphones, which represent a greater digital identity risk than basic cell phones. Whereas basic cell phones track cell tower positioning, call and text numbers, times, and durations, smartphones track that data and more, including: GPS positioning, Wi-Fi positioning, app data, Internet browsing history, collected and shared multimedia, and account credentials.

Only one percent of teens have no phone or Internet-enabled device; 95 percent of teens have at least two. Due to teens' ubiquitous usage of mobile devices and how much data they potentially collect and share, smartphones are creating digital footprints for teenagers at an unprecedented rate.





In addition to Internet browsing, teens make and maintain Social Network Service (SNS) accounts: 93 percent of teens have accounts on at least one SNS, and 71 percent use multiple sites.

Although the exact PII shared depends on the site or app used and the actions of an individual teen, popular online activities among teens share the following general types of PII.

PII Shared through Apps and Activities (*Pew Research Center Data)

App/Activity	% of Teens*	Typical PII Shared
SNS	93%	• Full name • DOB • Location • School • Interests • Email • Phone number
Online or App Gaming	72%	• Email • Phone number • Gaming handle • In-game activities • Interests • General location
Video Call/Chat Apps	47%	• Online handle • VOIP phone number • General location • Live video feed
Frequent Texting (>30 messages/day)	47%	• Phone number • Location (to provider)
Messaging Apps	33%	• Email • Phone number

The Traditional Teen Identity Milestones: Driving and Working

According to the Centers for Disease Control and Prevention's 2013 analysis, 76 percent of high schoolers

drive. Many teenagers not seeking a learner's permit or driver's license will obtain a state-issued identification card to use when flying, filling out W-4 tax forms, or voting. Obtaining these documents requires submitting proof of identity and address to state government officials. Depending on the state, the required proofs and PII include:

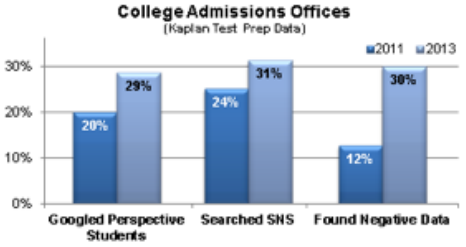
- Full name
- DOB (and proof of age)
- SSN
- Affidavit signed by parent indicating residence
- Direct bills in teenager's name

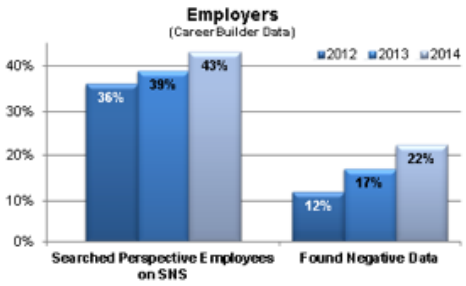
Visiting a state's motor vehicle office is often the first time individuals attempt to prove identity to government representatives, and therefore may be the first time individuals receive an indication their PII was previously stolen and used for identity theft. However, indications will not always appear at this point. Depending on the intent of the identity theft (e.g. opening new bank accounts, obtaining false government identification, or taking out loans), evidence may not appear until the victim requests a credit report or receives a rejection of a tax form filing, state identification, or passport application.

Driving introduces many additional identity related records. Depending on the state, vehicle ownership status, and driving record these include:

- Vehicle registration (name, phone number, address, license number, vehicle information, lease/lean information, planned car usage)
- Personal property taxes (name, address, vehicle registration)
- Civil fines and penalties, i.e. speeding tickets (name, address, vehicle registration)
- Insurance (name, address, license number, vehicle registration)

Nearly a quarter of high schoolers hold jobs, according to 2014 US Bureau of Labor Statistics data. Applying for jobs includes putting resumes online or sending potential employers your name, address, phone number, and email; putting your PII in the hands of many individuals. Depending on location and age, work permits may be required after receiving a work offer. These permits necessitate supplying PII to the state, including name, address, DOB, phone number, employer information, and job specifics.





A job means paychecks, which require bank accounts, prepaid cards, or using check cashing stores. Depending on the method chosen, the teenager may need to share PII, which may include: citizenship, SSN, DOB, name, address, phone number, email, job information, employment and address history, or merely a state issued photo identification. Identity theft victims can become aware of the theft during job applications or when filing income tax returns.

Threats beyond Identity Theft

As teens expand their online presence and digital identity, new threats affect Internet and social media usage. Posting PII increases the avenues available for identity theft, but other types of posts can also threaten teens. Information and media posted online can become a permanent gallery highlighting an individual's digital identity. Poor online decisions made by a minor can have lasting repercussions throughout that person's life.

This data can also be used to lay criminal charges against teens or their families, potentially including:

- Child pornography charges for "sexting"
- Cyberbullying charges for posting or spreading excessive malicious information
- Hate crime, malicious harassment, or intimidation charges for threatening or offensive comments inciting violence
- Drug and alcohol charges based on social media photos

This data can also leave a digital data trail influencing college and job applications for years. College admissions officers and hiring managers increasingly use Internet and social media searches to vet applicants, often resulting in rejections.

Teen Privacy and Voluntary PII Sharing

2013 Pew Research Center data shows teens are posting more PII to their SNS profiles, with the percentage posting:

- Cell phone numbers up from 2 percent (2006) to 20 percent (2012)
- Photos of themselves up from 79 percent (2006) to 91 percent (2012)
- School name up from 49 percent (2006) to 71 percent (2012)

Despite increased data sharing, teens are aware of privacy concerns. About 70 percent having sought advice on managing online privacy. Teenagers should be encouraged to continue reviewing and enabling account privacy settings.

Teens are Conscious of Privacy Concerns (Pew Research Center Data)	
Among Social Media Users	• 60% limit Facebook profiles to Friends • 25% limit Facebook profiles to Friends of Friends • 24% restrict their tweets
Among App Users	• 51% avoid downloading apps due to privacy concerns • 46% have turned off location tracking features • 26% have uninstalled apps due to excessive PII collection

Other Avenues of PII Sharing

Additional possible avenues for teens to share PII include:

- Special interest club or sports involvement
- Shared or self-owned bank accounts and credit/debit cards
- Passport applications (used for study abroad or vacations)
- Inadvertent sharing through improper disposal of PII-containing documents

As mentioned in the Public School (5-to-8) and Pre-teen (9-to-12) articles, special interest clubs and sports teams can publicly list membership rosters (revealing name, age, and general location) and photos (including tagging individuals). Credit and debit cards generate spending records tracked by banks and some stores. Parents should continue monitoring these PII leakage avenues and begin involving teens in managing this data.

Although parents can obtain passports for children at any age, teens 16 and older can apply for US passports using their own documentation. Obtaining a US passport requires submitting the following PII: proof of US citizenship (e.g., a certified US birth certificate or certificate of naturalization), proof of parental awareness (e.g., a parent's check for paying fees), and photo ID (e.g., a valid US driver's license).

Proper disposal habits of PII-containing documentation should be ingrained in teens, especially as the number of documents will only increase over time: paycheck stubs, test results, car titles, expired credit/debit cards, bills, and other records. These documents should be stored in a safe, limited access location when needed for future reference. When necessary, they should be disposed using a crosscut shredder. Many communities sponsor shredding events where residents can bring in documents and mail for on-site shredding; check your local community bulletin or news channel website for upcoming events.

Conclusion

The teenage years, which often see a great expansion in digital presence and the creation of PII documents, present unique challenges in today's digital world for mitigating PII sharing, managing digital footprint and reputation, and reducing identity theft risk. The first goal is understanding all potential PII sharing avenues (necessary, voluntary, and inadvertent) so mitigating steps can be taken.

Always be careful of oversharing PII online - regardless of the venue - and whenever possible restrict privacy settings. Remember, once data is online, it is online forever. Even so, asking individuals and organizations to remove photos, tags, mentions, and links to one's digital identity can mitigate risk.

Managing PII and mitigating identity risks can only go so far in protecting individuals from identity theft. In addition to following guidance on minimizing PII sharing and protecting PII, all teens should monitor their credit reports, especially once they obtain credit cards or car/student loans. Monitoring your credit reports can be done for free at Annual Credit Report (https://www.annualcreditreport.com/).

THE COLLEGE YEARS: INDEPENDENCE LEADS TO NEW THREATS

By adulthood, you are out of your parents' house—or want to be—and are ready to establish your own identity. But if you are like most young adults, the world already knows a great deal about you. Maybe too much.

Most individuals over 18 have well-established digital identities, complete with high school diplomas, driver's licenses, extensive activity on social networking services (SNS), multiple employers, and bank accounts. The digital footprint for young adults grows even larger as they attend college, vote, join the military, get apartments, work, get married, and pay taxes.

The years following high school are the first in which individuals develop broad identities that are distinct from their parents. For that reason, the variety of new records, the amount of PII collected, and the potential risks are substantial.

Voter registration
Registering to vote is a key milestone in one's life. Applications vary by state but typically ask for name, address, date of birth (DOB), political party affiliation, and driver's license number. If applicants do not have driver's licenses, they may be asked for the last four digits of their Social Security numbers (SSNs). A few states require the full SSN. Application forms may also request gender, race, email address, and phone number, but providing that information tends to be optional.

Voter registration databases are public records, excluding driver's license numbers, DOBs, and SSNs. In some states, these databases are searchable online. Nationwide collection of the data for marketing and political purposes is routine, which makes this data particularly vulnerable. In 2015, a hacker discovered on the Internet a database of voter records for 191 million Americans, including addresses, DOBs, and phone numbers.

Some states allow "high-risk" individuals, such as law enforcement officers, crime victims, military personnel, and their families to request that their addresses and phone numbers be exempt from release.

Selective Service
Adult males, including non-citizens under 26, must register with the Selective Service System, which maintains a list of draft-ready individuals, e.g., males aged 18 and older. The application requests basic PII, such as name, DOB, gender, and address. The names and classifications of registrants are public and accessible by anyone.

Apartment
Independent-minded young adults may get their own apartments. Apartment applications require SSN, marital status, names of relatives, personal references, credit checks, and bank account information. If utilities are not included, renters must provide utilities companies with similar PII and financial information.

Apartment applications and leases are not public records, but information about individuals living at a particular address, including their ages and relationships, often can be easily obtained from online data brokers. These brokers compile information from public records, private companies, and online sources. Young adults should check the websites of data brokers and complete "opt out" forms to have their information removed.

College
Higher education applications require basic PII, including name, SSN, DOB, marital status, telephone number, email, race, gender, names of parents, and other information. There are two primary sources for PII:

- College Applications: Many colleges use the Common Application and Universal College Application, websites that allow students to enter information once—including school transcripts, SAT scores, reference letters, writing samples, and resumes—for submission to multiple schools. The service is convenient but poses a risk if passwords are compromised or the system is hacked. Passwords should be difficult to guess and never shared.
- FAFSA: Completing the Free Application for Federal Student Aid, or FAFSA, is necessary to apply for government aid, student loans, scholarships, and grants. Some required PII includes name, SSN, DOB, marital status, driver's license number, address, parent names, parent incomes, and parent SSNs. The form asks questions about student and parent incomes, financial accounts, assets, and receipt of public assistance. The information can be entered online and is accessible by selected colleges and government agencies.

Federal law protects student privacy, but with permission their PII may be shared with dozens of entities. Students should review the privacy policies of organizations when seeking scholarships and request that colleges not use SSNs for identity purposes.

Jobs
The job search process can involve placing extensive PII on websites and in the hands of many potential employers.

- Job applications: Whether online or a hard copy job applications seek basic PII, complete work histories, schools attended, past salaries, and personal references. Most applicants include a resume and cover letter, both of which may contain additional biographical information, including hobbies and group memberships.
- Online job sites: Individuals can register for websites that compile job listings or allow them to create profiles to market themselves to employers. The shared PII mirrors what is typically provided on job applications and resumes, though users may provide more detail than is given on paper applications.
- Taxes: Since many adolescents do not have to file tax returns, most young adults are dealing with the Internal Revenue Service for the first time. Tax returns require an individual's name, address, SSN, employers, wages earned, and other PII. Individuals may share this information with accountants to prepare returns, websites that let users prepare returns online, or tax preparation software.
- Commuting: If a commute involves toll roads or bridges, an individual may sign up for EZ-Pass, providing the service with a name, address, credit card, driver's license, license plate, and type of vehicle.

Credit cards
About half of college students receive credit card offers on a daily or weekly basis, according to the US Department of Education. Many students take advantage of the offers, providing companies with basic PII, the names of employers, income, and credit reports. Credit card applications, particularly pre-approved offers, should be shredded before they are discarded, and young adults should closely monitor credit reports for suspicious activity.

Personal computing
Young adults are heavy users of smartphones, SNS, unprotected computers in libraries, and public Wi-Fi hotspots. Careless digital behavior can make it easier for scam artists and identity thieves to gather information.

- Smartphones/computers: Many of the websites young adults use to find free music and games are often havens for malware. Once installed on a device, malicious software can log keystrokes and steal personal information. Students should use reputable websites for entertainment and be cautious when installing software. Personal devices should always be password-protected.
- Websites/blogs: Many young adults create personal websites or blogs, sharing a great deal of information about their finances, employers, families, friends, and life events, such as birthdays.

Military
Joining the military requires divulging an enormous amount of PII, some of which may become public immediately, or at some point in the future. Each of the five military branches has different enlistment requirements, but all seek common PII from recruits, including name, address, SSN, DOB, education levels, and SAT/ACT scores. Information may also be recorded from a Social Security card, birth certificate, and driver's license. Recruits are fingerprinted and must submit to background checks.

A service member's complete military record is available to their next-of-kin. Most military records are exempt from Freedom of Information laws but some information about service members can be requested by anyone, including name, positions, titles, salaries, grades, locations, training, and awards.

Military members can request an active duty alert on their credit reports to guard against fraudulent activity. The alerts last a year and require businesses to verify an applicant's identity before issuing credit.

Be vigilant
College-age adults are the biggest targets for identity

theft, losing on average $1,246 per incident, the highest of any age group, according to a survey by Javelin Strategy and Research. Few are financially savvy—the survey noted that young adults on average take three months to detect identity theft—and many fail to properly secure, or dispose of, private documents.

With the abundance of new PII, and increased opportunities for it to be abused, young adults need to be hyper-vigilant about safeguarding sensitive information.

DECADES OF IDENTITY RISK

Working adults experience many major life events—such as buying homes, starting businesses, and having children—that require sharing a lot of personally identifiable information (PII), exposing them to increased risk of identity theft. Nearly 14 million Americans between 25 and 64 were victims of identity theft in 2014, up from 9 million in 2008, according to the Bureau of Justice Statistics.

22 to 25

CAR

LICENSING

SOCIAL MEDIA

Your first real identity risks often come from buying a vehicle or getting a professional license or certification. The information is generally basic but still sensitive. Social media opens you to revealing photos, names of partners and even sexual preferences.

25 to 40

MARRIAGE

CHILDREN

MORTGAGE

Getting married and starting a family often includes marriage licsenses that are public and PII being made for your child. Mortgages include highly sensistive financial information and are often made available to dozens of inidiviuals and agencies.

40 to 55

DIVORCE

ENTREPRENEUR

BUSINESS PLANNING

Divorce filings may be made public but can be sealed. Details are often highly sensitive. Business paperwork as an owner or entrepeneur generate a large amount of PII both on you and the business as an entity.

55 to 65

SELLING HOME

RETIREMENT ACCOUNTS

Property sales and retirement accounts require and generate significant amounts of PII, some of which may be publicly available.

Sources: National Center for Health Statistics, The Kauffman Foundation, Identity Theft Resource Center, Bureau of Justice Statistics

THE WORKING YEARS: HOW TO KEEP YOUR IDENTITY SECURE THROUGHOUT YOUR WORKING LIFETIME

You're all grown up, finished with college, comfortable in your job, thinking about starting a family, and planning to spend the next few decades dodging an avalanche of risks to your identity.

Wait, what?

You read that right. Working adults have a digital footprint spanning roughly 43 years, from the typical college graduation age (22) to the common retirement age (65). This stage includes many major life events, including buying a first home, having children, starting a business, and planning for retirement. It is also the time when individuals make the most contributions their digital footprints. The broad range of activities one conducts during this period brings many risks and requires careful planning to manage them.

EMERGING ADULTS (22 TO 25)

After getting an apartment, a process covered in the previous article on Young Adults, often the first thing on the list for emerging adults is buying a car. This transaction will require individuals to provide a great deal of personally identifiable information (PII) to car dealers, banks, insurers, and their states of residence. Automobile purchase agreements, loan applications, vehicle registrations, and insurance policies all require similar information: name, date of birth (DOB), Social Security number (SSN), address, gender, driver's license number, type of vehicle, and vehicle purchase price. Loans require additional PII, including income, living expenses, and name of employer.

At the workplace, PII may also be shared with outside companies that manage 401(K) plans, medical, and other benefits. Additionally, many jobs require government licensing or professional certification. Occupational licensing varies by state, but most require applicants to provide a moderate amount of PII, including name, address, SSN, DOB, telephone number, and proof of competence (work or education history). In most states, licensing records are public and accessible online, though sensitive PII is not disclosed. Certifications, granted by professional or trade groups, require similar PII.

Socially, emerging adults share a great deal of information on social networking services (SNS) and online dating websites. That PII can include biographical information not easily obtained elsewhere, including photographs, names of partners, locations frequently visited, religion, and sexual preferences.

The primary risk in this age group is carelessness in managing digital and physical records. Emerging adults can avoid risks to their identity by:

- Using strong alphanumeric passwords unique to each website and electronic device.
- Signing up for electronic statements for financial and benefits accounts.
- Being cautious when sharing personal information online.
- Properly shredding financial documents and other records with PII.

STARTING A FAMILY (25 TO 40)

On average, most adults in the United States are married for the first time in their late 20s (27 for women, 29 for men), according to the Pew Research Center. Those who decide to get married will apply for marriage licenses, providing their names, addresses, SSNs, occupations, DOBs, places of birth, names of parents, and previous marriages. Depending on the state, marriage licenses may be public records. Gift registries and wedding announcements may also contain biographical information, and may be accessible online.

The average age of a first-time mother was 26 in 2014, according to the National Center for Health Statistics.

Having a child necessitates sharing PII with hospitals and government agencies. Newly created documents include medical records, birth certificates, Social Security card applications, and government benefits. See "From the Womb to Preteen" on Page 4 for more details on PII created at birth.

Individuals, on average, buy their first home at 33, according to Zillow, an online real estate marketplace. The process of obtaining a mortgage is almost forensic in nature, with banks, real estate agents, and local, state, and federal government agencies closely examining applicants' finances, work history, credit reports, tax returns, and other documents. The PII required is substantial, including:

- Pay stubs for all applicants
- W-2 tax forms
- Names and address of employers
- Bank statements
- All sources of income (wages, pensions, Social Security, alimony, child support, investments)
- Information on all debts (car loans, student loans, credit cards)
- Assets (property, stocks, life insurance policies)

Some or all of that information is shared with a dozen or more individuals and organizations necessary to complete the purchase process, including lawyers, home inspectors, appraisers, land surveyors, title companies, public utilities, government officials, and insurers. Individuals should check with all parties to discuss how PII is stored and protected.

After a home purchase is completed, certain documents become public record and, depending on the municipality, may be easily accessible online. The mortgage document contains the closing date, name of the borrower, name of the lender, property address, and loan amount. Property tax bills and liens against the property are also public.

Mortgages are a rich target for identity theft with scammers stealing PII to fraudulently purchase properties or impersonate and transfer deeds to themselves, or others.

Homeowners should safeguard all mortgage documents and use strong alphanumeric passwords for online accounts. Regularly checking credit reports is recommended as is occasionally checking with the local municipality to ensure the property deed has not been transferred.

MID-LIFE (40 TO 55)

The National Center for Health Statistics estimates that nearly half of marriages will last fewer than 20 years. That means a large number of middle-aged adults will experience divorce. Divorce filings include a large amount of PII, including personal and financial records, as well as information about children, and intimate relationship details. Depending on the state, some divorce records may be public, though parties can request they be sealed. Any specific filings involving children typically are exempt from disclosure.

The rate of PII-sharing continues to grow as many individuals in this age group focus on accumulating wealth, making more investments, and starting businesses. The average age for entrepreneurs starting their first businesses is 40, according to The Kauffman Foundation. Founders must file certificates of incorporation with their states, which typically ask for the business name, mailing address, and a company director. Depending on the business, individuals may have to file a business tax return in addition to a personal return.

As with personal taxes, a thief can file a fraudulent return using a company's name, address (readily available in state filings), and a stolen federal Employer Identification Number. Business credit reports also contain PII, including names of owners, banking relationships, and information from public records. Business credit reports are more widely available than personal reports.

Loans from the Small Business Administration are public record and searchable online. Information provided includes business name, address, and loan amount.

Business owners should safeguard tax information and regularly check business credit reports for suspicious activity.

PRE-RETIREMENT (55 TO 65)

Pre-retirement years typically focus on asset accumulation, debt reduction, and estate planning.

- Tax-advantaged accounts: Many individuals open Roth IRAs, or SEP IRAs for the self-employed, to accumulate savings. As with most financial instruments, a significant amount of PII is required, including name, address, telephone number, SSN, DOB, employer information, bank account number, brokerage account number, driver's license number, country of citizenship, and names of beneficiaries.
- Home sales: Some individuals seek to reduce expenses by selling their primary home before they retire. The sale of any property generates substantial PII, some of which will be public record. The rules for home sales vary by state but they typically include a sales contract that includes the terms of the deal and property disclosure form that lists all of a home's defects. At closing, additional documents are signed and transferred to the new owner, including the property title. The sale is recorded by the municipality and a satisfaction of mortgage is filed, which lists the mortgagor, amount being paid off, and seller's name. In most states, land records are public, including the satisfaction of a mortgage.

Older workers, who may not be as diligent about online and computer security, are particularly vulnerable to identity crimes. They should continue to monitor their credit reports for suspicious activity, especially when making or contemplating major life changes.

As working adults age, keeping identities and finances secure takes more effort. Nearly 14 million Americans between 25 and 64 were victims of identity theft in 2014, up from just over 9 million in 2008, according to the Bureau of Justice Statistics. The increased sharing of PII, higher incomes, and number of financial accounts in this age group inflate identity-related risks. Safeguarding PII, closely monitoring financial accounts, and limiting SNS exposure greatly reduces the likelihood of becoming a victim.

RETIRE AWARE: HOW TO PROTECT YOUR IDENTITY AFTER RETIREMENT

You've made it to retirement! Working to earn your living is no longer a necessity. Instead you're now using carefully curated savings, retirement plans, and possibly pensions or social security as your sources of income. Living a on a fixed income in a continually changing technological landscape presents a whole new set of challenges, as does navigating government applications and housing changes.

Technology Changes

Technology is rapidly changing at a pace that continues to increase. Individuals turning 65 in 2016 were born in 1951, which means they experienced an emergence of new commercial technologies. Within their lifetimes, a retiree has experienced the adoption by most households of, color television, cable television, and television recording mechanisms, according to Dow Jones & Company. Personal computers and cellular phones weren't widely commercially available until the early 1980's, when today's retirement-age adults were already in their 30s. The Internet wasn't widely commercially available until they were in their 40s.

As adults aged 65+ adopt new technologies, they can find themselves particularly vulnerable to identity theft and fraud if they apply outdated levels of caution to current problems. The extent of data available today through digital footprints is unprecedented: whether legally to advertising companies tracking web browsing history, or e-commerce companies tracking purchase history; or illegally through a hacked email account. Indeed, email accounts are particularly vulnerable as they have the ability to reset passwords for nearly all online services used, granting

direct access to data, both financial and PII. For individuals not well
versed in today's technology, the scope of this threat can be overwhelming.

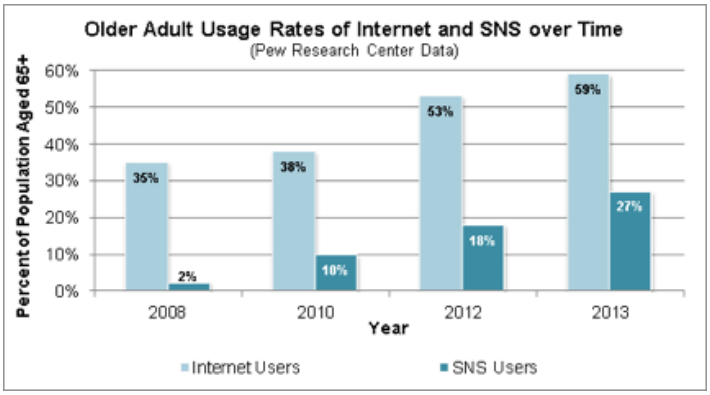
Digital security and privacy is becoming increasingly important to adults aged 65+, as more individuals use the Internet and Internet-capable devices. Adults aged 65+ generally adjust more slowly to changing technologies than younger adults, but Internet and SNS use is still increasing among this age group. As of 2015, 61 percent of Americans aged 65+ use the internet.

Despite slow adoption rates, 34 percent of all 65+ adults use social networking sites as of 2014. Among these adult SNS users, Facebook is the primary site used.

SNS Sites Used by Older Adults (Aged 65+)
(Pew Research Center Data, 2014)

Site	% of Internet Users	% of 65+ Population	Typical PII Shared
Facebook	56%	34%	• Full name • Date of Birth • Location • School • Interests • Email • Phone number
Twitter	10%	6%	• Name/screen name • Email • Location
Instagram	6%	4%	• Name/screen name • Email (or phone number) • Location

Fewer older adults use smartphones, with only 18 percent of individuals aged 65+ owning one compared to 55 percent of all adults (Pew Research Center data, 2013).



And unlike teens, smartphone adoption among older adults isn't skyrocketing: adoption rates have increased from 11 percent (2011) to 18 percent (2013). Often the portable digital device used by older adults is a tablet or e-reader, preferred due to larger display and adjustable text size; tablets and e-readers have a combined adoption rate of 27 percent (2013).

Locking all Internet-capable devices with strong passwords is a good first barrier, but is insufficient to protect an individual against identity theft and fraud. Privacy restrictions are needed on all online accounts, and individuals should be careful in choosing what information they post online. Once information is available online it becomes part of your permanent digital identity. The old adage still applies: think before you post.

Applying for Medicare/Social Security

Retirement-age Americans can apply for numerous federally sponsored programs, including Medicare and Social Security. These processes require a long checklist of documents and information. In general, the PII required for applying includes:

- Birth information (date and place)
- Current health insurance information (employment information and name)
- Marriage and divorce information (names, dates, SSNs, and locations)
- Employment and military service history

These services are increasingly moving online, shifting PII sharing from paper documents at local field offices to the Internet. Although securing the information you enter during online applications is the responsibility of the federal agency hosting the site, three responsibilities fall to the individual:

- Ensuring your login credentials are strong, secured, and known only to you
- Ensuring you maximize security controls for resetting credentials
- Ensuring you only access the legitimate government website (rather than fraudulent sites made to gather PII)

When accessing online services that involve sharing significant PII, know the correct website and type the address to access it directly into the address bar. Following email solicitation links and third party website links can re-direct you unknowingly to fraudulent websites.

As you approach 65 years old, an increasing number of companies and scammers will compete for your attention and money by mailing you special applications for benefits and services or calling you to inform you of time-sensitive benefit opportunities. Approach these offers and calls carefully. You will be best served by doing your own

research and finding out the facts about these government benefits through the Social Security Website (https://www.ssa.gov/), Medicare website (https://www.medicare.gov/), or asking questions at your local Social Security Office.

Changes in Housing

When determining your funding sources and living costs in retirement, considering your housing situation is vital. Depending on circumstances you may consider selling or transferring your home, taking out a reverse mortgage, or moving into an age-restricted community. Each of these choices requires the collection and presentation of significant PII.

PII required typically revolves around name and address, plus some financial details, and much of this data is public record, as discussed

in The Working Years: How to Keep Your Identity Secure Throughout Your Working Lifetime (Page 12). At least some of this data will need to be shared directly with the following individuals: real estate agent, buyer, the buyer's real estate agent (post offer acceptance), lawyers drawing up paperwork, title search company, escrow company, mortgage company, home inspections company, and a tax professional for capital gains filing help.

In particular, reverse mortgages can be complicated. A lot of erroneous, fraudulent, or misleading information is circulated relating to reverse mortgages. As with Social Security and Medicare, many scammers will specifically target older adults with fraudulent schemes framed around reverse mortgages. According to the FBI the number of reverse mortgages issued has grown over 1,300% since 1999. As these transactions become more typical, they create an increasingly large target niche for fraud.

Ensure that you have the full and accurate facts about reverse mortgages before signing any paperwork. Do your own research on types of reverse mortgages directly at the FTC's website: https://www.consumer.ftc.gov/articles/0192-reverse-mortgages. You can also visit the US Department of Housing and Urban Development's website for a list of HECM counselors, or call the agency at 1-800-569-4287. Do not rely solely on advertisements, phone calls, or chance meetings with strangers. And be cautious of fraudulent websites designed to mimic legitimate ones for collection of your PII.

Threats and Scams

Changing technology creates new identity theft pathways and vulnerabilities. Although theft of mail and trash, along with phone scams, are still used by criminals, other new avenues include hacking and spearphishing, or using e-mail and other electronic means to lure individuals into divulging PII. Financial abuse and crimes extorting or stealing money from older adults are a growing problem, estimates indicate that these crimes against Americans aged 65+ result in a loss of $2.9 billion (2010 MetLife study) to $12.76 billion (2015 True Link study) per year.

Financial scammers will try to play on vulnerabilities that come with age: fear of forgetting, fear of losing control of your house or finances, concerns over leaving an inheritance. Be vigilant. For a review of various common scams used to target older adults, what to watch out for, and how to report suspected or actual scams, visit the FBI's website: https://www.fbi.gov/scams-safety/fraud/seniors.

Conclusions

The golden years involve trying to settle into a peaceful retirement, all while facing targeted fraud attacks, navigating government-sponsored programs, and adjusting to the ever changing technology landscape. Increasingly the services you use will be available online: whether it is applying for Medicare and Social Security, researching reverse mortgages, banking, or shopping. When transitioning to digital services, it is vital to follow good privacy and security practices. Checking privacy and security settings on your online accounts is just like shredding documents containing PII. Take the time to review the most up-to-date DoD SmartBook for detailed instructions on using social media and the internet safely and securely.

You best defense against threats and scams at any age is knowledge, skepticism, and a dose of common sense. Remember: if it seems too good to be true, it probably is.

HEALTH RECORDS: MAINTAINING A HEALTHY DOSE OF PRIVACY AND SECURITY

The compromise of health records is especially damaging to your personal security. Not only can criminals steal sensitive personal and financial information from these documents, but they can also access private information about your medical history, treatments, and other information you have shared with your doctor in confidence. This information could be used to embarrass you, threaten you, or even to deny you effective medical treatment. With the rise of modern genetic testing and analysis services such as 23andMe, hackers may even be able to steal your entire DNA sequence.

The increasingly electronic nature of the healthcare industry has opened the door to a variety of new privacy and security threats. In particular, phishing scams and the compromise of Electronic Health Records (EHRs) pose a threat to individuals.

Phishing Scams

A variety of phishing scams, which are attempts to acquire sensitive information such as passwords or credit card details while impersonating a trustworthy person or entity, have targeted people seeking to buy health insurance. Increasingly, spammers and hackers attempt to steal financial and personal information while posing as employees of insurance providers. Frequently tied to organized crime groups, these malicious individuals may attempt to contact you via email, phone, or text message and solicit your PII.

To prevent becoming a victim of these scams, only use health insurance providers located on official health insurance exchanges, such as Healthcare.gov. In addition, be wary of health insurance providers claiming to offer extraordinarily low prices or low premiums. When in doubt about the validity of a communication from a health care provider, call the official number provided on your health insurance card or on the provider's website. Further, if you purchased insurance via your employer, contact an HR representative to verify the authenticity of the suspicious communication.

Electronic Health Records

The tools used to provide healthcare and health insurance are changing in the United States today. Electronic health records (EHR) allow your health care and health insurance providers to rapidly retrieve and share your healthcare information. EHRs facilitate communication between patients and health professionals. Whereas paper records were only available to a single user at a time, EHRs allow multiple users to access your health information simultaneously. Easier edits and updates can improve the accuracy of information.

Despite the many advantages of EHRs, they come with a variety of privacy and security risks that could compromise the personal information of you and your family. Similar to other kinds of electronically stored data, EHRs can be compromised by hackers or shared with third parties without your knowledge. In addition, the numerous ways we communicate with health professionals via mobile devices, mobile applications, computers, email, text messages, and on public WiFi networks could make that information vulnerable to typical privacy risks.

To protect yourself and your family when accessing EHRs, use the same guidance as applies to protecting yourself on computers, mobile devices, and when browsing the internet. Enable access controls such as passwords or PINs, encrypt information and enable HTTPS when possible, and avoid sending personal information to health insurance companies over public WiFi networks.

ONLINE IDENTITY AFTER DEATH: THE GHOST IN THE MACHINE

When individuals die, their digital identities expand rapidly as police departments, courts, hospitals, churches, and government agencies respond to the death, and once-private records become public.

Typically, by the time people pass away, their lives are flush with digital records from birth, education, employment, marriage, finance, and military service. A large number of additional records are created post-mortem, and the personally identifiable information (PII) they contain continues to pose a risk. The identities of an estimated 2.5 million deceased individuals are stolen annually, according to the Internal Revenue Service.

Here are some common post-mortem records and tips to safeguard a loved one's PII:

Death certificate: The information collected varies by state, but most death certificates list full name, address, Social Security number (SSN), date of birth (DOB), marital status, race, occupation, and names of parents. In most states, death certificates are only provided to immediate family, legal representatives, or others with a legitimate financial, or public policy interest. However, in some states, death certificates or indexes of recorded deaths may be open to public inspection and made searchable online.

To protect the identity of the deceased, deaths should be reported to companies and government agencies as soon as possible. Among them:

- Banks, insurers, and credit card companies should be notified of the death to safeguard or close financial accounts. Most institutions will mark accounts as "Closed: Account Holder Is Deceased" to guard against fraud.
- Credit reporting agencies, such as Equifax, TransUnion, and Experian, should be contacted and asked to place a "deceased alert" on the credit file. After a few weeks or months, ask for a copy of the report to check for suspicious activity.
- Department of Motor Vehicles offices should also be contacted to cancel driver's licenses; this process will vary by state.

Police report: The police often prepare reports detailing the circumstances of a person's death. These reports contain the deceased's name, address, DOB, spouse, relatives, addresses, and other PII. If a death is found to be a crime or suspicious in nature, the police will conduct an investigation and create more detailed reports.

In most jurisdictions, police reports are public and can be viewed upon request. However, state laws exempt some police records from disclosure and reports on active investigations may be withheld.

Autopsy: If requested by relatives or required by law, an autopsy may be conducted by a hospital or a municipality's medical examiner. The examiner determines the cause and manner of death and issues a report detailing their findings. These reports include name, address, medical conditions, height, weight, race, occupation, personal physicians, relatives, military service, and next of kin.

Most states allow access to some or all autopsy records, but may limit the release to government officials, immediate family members, and legal representatives. Some states only release an individual's name along with the cause and manner of death. In others, autopsies are classified as medical records and are exempt from disclosure.

Social Security: The Social Security Administration collects information on deaths for its records and to provide services and benefits to surviving relatives.

- Death Master File: The administration maintains a national database of deaths, though it is not comprehensive. The entire database is public record and contains names, SSN's, DOBs, and last known residences. Several websites allow users to search an index of the records.
- Social Security Account: A password-protected online portal allows individuals to access a personal statement containing their earnings records and estimates for retirement, disability, and survivor benefits.

Upon death, some Social Security records are open to the public. Anyone (for a fee) can request a copy of a deceased individual's original application for a Social Security Card, which includes name, DOB, place of birth, address, citizenship, race, gender, and names of parents. Identity thieves can also illegally purchase SSNs from online brokers.

Deaths should be reported to the Social Security Administration as soon as possible to guard against misuse of SSNs.

Obituary/Funeral records: Included in newspapers and funeral programs, an obituary may contain sensitive PII, including age, occupation, employers, place of birth, DOB, names of relatives, and other biographical information. Many websites allow users to search obituaries.

To guard against identity theft, consider limiting the information in the obituary. Use age instead of DOB. Also, if possible, do not include the mother's maiden name, commonly used by creditors, or any addresses.

Probate: The legal process of determining the distribution of a deceased individual's assets, known as probate, produces voluminous records. The court records—wills, financial accounts, insurance policies, and other directives—contain nearly every piece of an individual's PII, including land ownership, lists of personal property, relatives, current and former spouses, religion, and military service.

An individual's debts and other legal matters are also resolved during probate and may result in additional records with PII being created. Probate records, like most court documents, are public and, in some cases, can be accessed online.

Computers and online accounts: Upon death, family members may be able to obtain court orders to procure passwords for electronic devices and online services, such as iPads, email accounts, and social networking services. If access is granted, family members should consider limiting the amount of biographical information in the accounts or deleting them entirely.

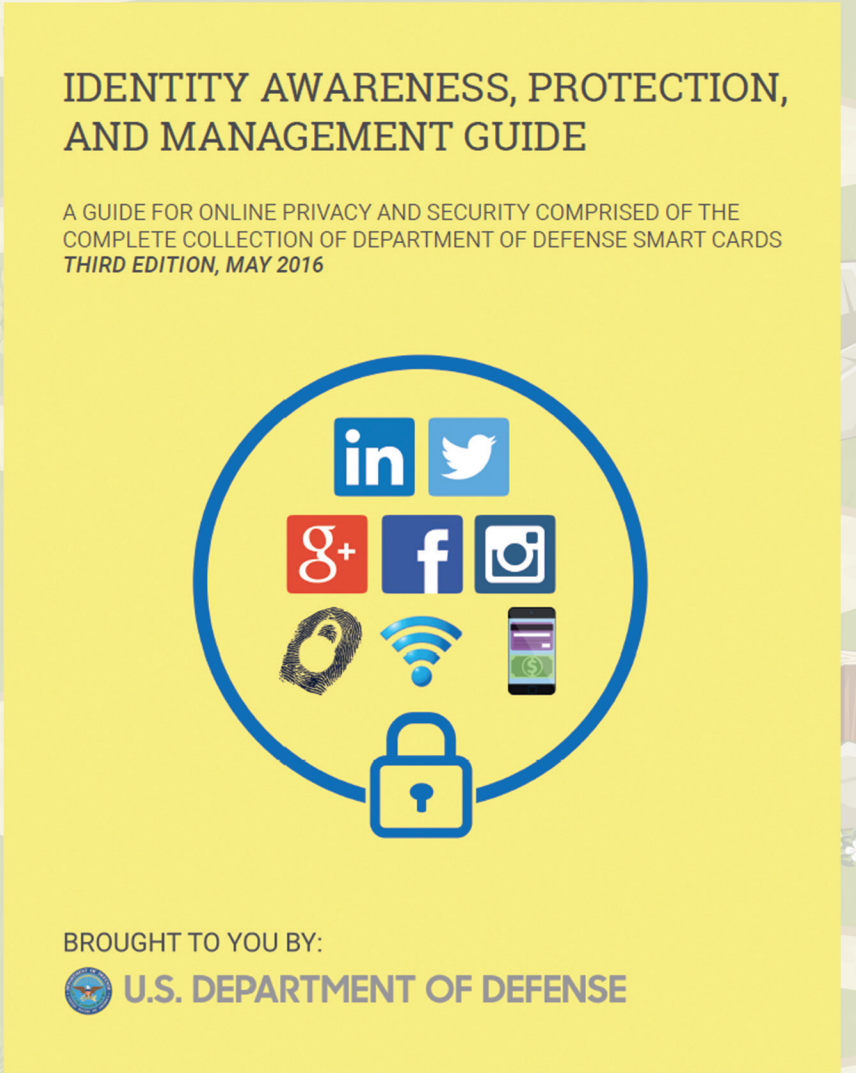
In some instances, online services will not allow anyone to access the accounts of deceased individuals, but they have other methods of restricting activity. For instance, Facebook does not provide passwords to a deceased person's account, but allows family and friends to request it be "memorialized," which keeps it online and allows them to share memories and save pictures. Login attempts are blocked on memorialized accounts. Immediate family members can also request that Facebook delete accounts of deceased individuals.

Census: The government releases US Census records 72 years after the date of the census. The records contain detailed information about an individual's family, occupation, income, education, addresses, personal property, living conditions, land ownership, and a trove of other PII.

The length of time before public release makes it so that most census records are not available until after an individual's death. However, individuals named on the records, their legal heirs, and their legal representatives can access census records at any time. After death, this right of access is extended to executors of an estate and an individual's beneficiaries named in wills and insurance policies.

Post-mortem identity theft is a growing problem. With the varied sources of data available on- and off-line, clever thieves can run up huge debts, causing additional stress for families, financial strain, and even delayed inheritances. Protecting the PII of a deceased family member is not something most people think about but it should be.

This issue is a good starting point for managing and protecting your family's identity. For more detailed information, please check out the Identity Awareness, Protection, & Management Guide.



Send an email to this address to get your copy!
OSD.NCR.OSD.MBX.DODSMARTCARDS@MAIL.MIL