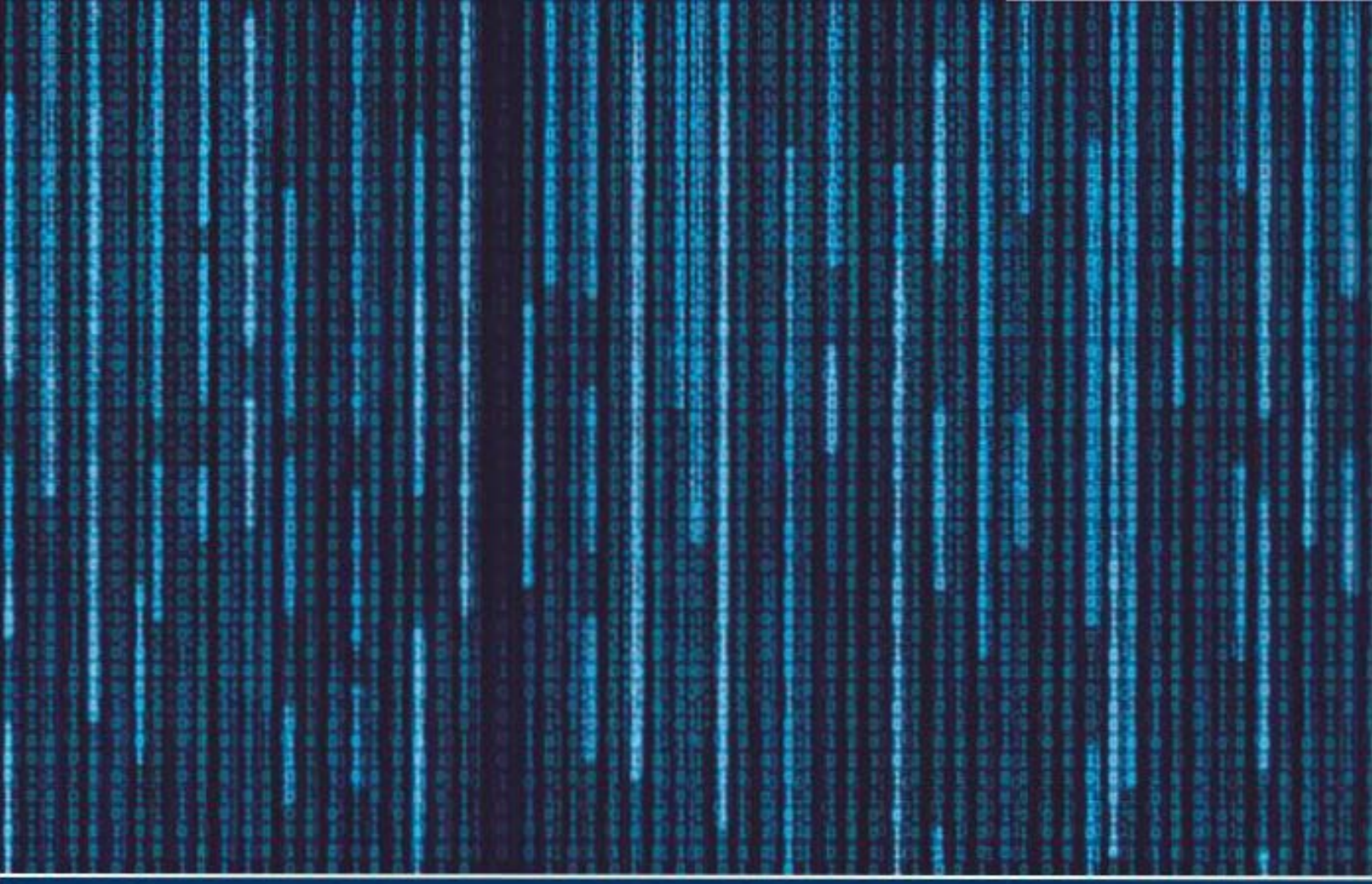

Digital Footprint:

Assessing Risk & Impact

18 February 2014

Homeland Security

National Cybersecurity and Communications Integration Center

Table of Contents

Executive Summary

To facilitate efficiency and effectiveness on a global scale, massive amounts of data are stored and processed in systems comprised of hardware and software. Each digital transaction or interaction we make creates a digital footprint of our lives. Too often, we don't take the time to assess not only the size of our digital footprint, but what risks are involved in some of the choices we make. Our data lives in our social media profiles, mobile devices, payment accounts, health records, and employer databases among other places. The loss or compromise of that data can result in an array of impacts from identity theft to financial penalties, fines, and even consumer loyalty and confidence. This results in both a shared risk and therefore shared responsibility for individuals, businesses, organizations and governments. The following product is intended to facilitate awareness of one's digital footprint as well as offer suggestions for a unified approach to securing that data. This is not an all-encompassing product, but rather offers discussion points for all that hold a stake in the security of our data.

Digital Footprint: Assuming Risk

The rapid growth of new technologies continues to make accessing information and resources faster and easier. Though increases in convenience and efficiency are often obvious, it is important to be aware that the interactions between a user and the internet become a part of the user's digital footprint. A digital footprint, often classified as active or passive, refers to the traces left by a person's activity in the digital environment. Active footprints are those created when an individual intentionally releases information. Examples include posting information or images to social media sites like LinkedIn, Facebook and Twitter. Alternately, a passive footprint is one that is created when data related to an individual is collected without that individual actively or intentionally sharing the information. Examples include the public posting of court records, marketing sale of home addresses, collection of web-browsing habits, and even through comments or pictures posted by others to social media. While there are methods that can be used to limit or reduce an individual's digital footprint, there is no practice that can be used to delete it altogether.

A digital footprint is useful in some instances, such as the convenience of linking certain web accounts for online payments or allowing a site to 'remember you' which avoids entering user names each time someone wishes to log in. However, a digital footprint is also valuable to parties interested in monitoring their website traffic or for use in targeted advertising. During the course of normal web-browsing an end-user may notice that the advertisements being displayed align closely to items they have recently searched for or purchased. There are several methods by which end-user information is collected to specifically target advertising; some include:

- **Third Party Cookies** – Cookies are small data files that are placed on an end user's computer after visiting a website. First party cookies are from the actual entity that owns the website, which allows them to recognize your browser/computer when you return to their site. Third party cookies, however, may belong to ad agencies associated with the visited website. Ad agencies pay websites to allow them to place their cookies on the end-users system as they collect data on a user to form a record of browsing habits, computer settings, preferences and so on. This information is often used for targeted advertising.

- **Search Engine Marketing** – Most commonly used search engines analyze users search terms to determine which advertisements will populate within search results and which will appear in the paid space. Information and ads that have been paid to populate for specific end users will generally appear in the page margins.

- **Past Purchases** – Purchases made both online and in brick and mortar stores often result in collected information such as zip code and regularly purchased items. This information is then used to suggest products for your next purchase or offer coupons for items similar to those you have purchased in the past.

- **Profile information** – Information that users include as part of a social media profile may be used by ad agencies to display targeted ads.[1]

It is also important to reiterate that a digital footprint is not solely created behind the keys of a keyboard. In addition to information about an individual that may be collected in brick and mortar stores, the rapid adoption of mobile devices for use in everyday activity has exponentially increased individuals exposure to various databases and interconnected processing systems which may be both actively and passively collecting information. For example, many mobile applications (apps) request access to information or other apps in use on your phone including phone and e-mail contacts, call logs, internet data and device location.[2] In some instances, the app may not function if the end user refuses to allow access to additional data. Collection of the information often continues even when the app is not in use. For instance, global position system (GPS) options often continue to geo-locate mobile devices even when the device itself is powered on but not in use. The more access given to applications, particularly when access to additional information is not necessary for the app to function properly, expands the passive footprint. Users will likely remain unaware of where their collected information may eventually reside.[3]

Figure 1: Ways in Which a Digital Footprint is Created

Conveniences like public/shared Wi-Fi can also expand an individual's digital footprint. In addition to logging onto free or even temporarily paying for public Wi-Fi at airports and restaurants, multiple retailers have begun experimenting with using Wi-Fi enabled devices as a means to track customer behavior. This tracking allows retailers to locate patterns in customer movement throughout stores and can result in the retailer changing store layouts or even sending customized coupons directly to a user's phone based on the items they are viewing.[4] This tracking allows retailers to locate patterns in customer movement throughout stores and can result in the retailer changing store layouts or even sending customized coupons directly to a user's phone based on the items they are viewing.[5] As some users have selected the option on their mobile device to connect to Wi-Fi signals by default, offering free Wi-Fi allows retailers to gather data on an individual's behavior without them realizing it is occurring.

There are also aspects of the digital footprint that are never meant to be available to the public. When individuals shop at online retail outlets, file their taxes, or get admitted to a hospital, sensitive data about them is entered into various databases. Beyond names, addresses and phones numbers, this data can include social security numbers, credit/debit card information, and medical history among other

information. As this data must be collected in association with these activities, there is a threshold of assumed risk users engage in on a daily basis. While individuals assume this data is securely stored in an organization's backend database, the security mechanisms of these systems can and do fail at times. Whether these failures are the result of a misconfiguration, lapse in due diligence, or a malicious breach, once the information is exposed, unintended bread crumbs of one's footprint can surface in an unknown number of places.

The valuable pieces of one's digital footprint that live on these backend databases are often why they are the target of malicious activity. A media report from 7 August 2012 indicates that from 2009 to 2012 approximately 21 million patients had their medical records exposed in various data breaches which were reported to the federal government.[6] More recently, media reports have indicated the targeting of various retail point-of-sale (POS) terminals for the purpose of exfiltrating customer credit/debit card information. There are also multiple sources with our information that are less often considered when assessing one's footprint, such as when companies use third party vendors or outsource certain business functions. Employers require sensitive information to confirm an individual's right to work or to file taxes. This information may then be shared with third party companies as some or all human resources and tax functions can be outsourced, therefore expanding an employee's footprint. The same can be said in cases of payment information, as it is not only captured at a retail level but may also be processed by another vendor. Additionally, services may be rendered by a medical facility but bill payment is facilitated through a collection company. Individuals are fully aware of the name of their employer, the store where they made purchases and the doctor's office they visited, but less often are they aware of the third party companies that have also collected their information as a result.[7] Though we may be forced to accept some level of risk to participate in many daily activities, it is helpful to be aware of both your passive and active footprint in the event you must take steps to mitigate the potential impacts.

Consumer Impact: Risk Acceptance vs. Avoidance

In order to have more control over the risks of your sensitive data being exposed, it is important to asses one's digital footprint. Individuals may begin to assess their footprint by querying their own name in a search engine. Search engines use programs called spiders that crawl web content and catalog keywords.[8] Even information that has been removed from the web can still be found in a search engines cataloged cache. There are also various tools that can be used in this assessment such as like Pipl, Spokeo and 123people, which aggregate information about an individual. Tools like the WayBack Machine allow individuals to browse over 390 billion archived web pages dating back to 1996.[9] By entering a name and location, these engines can return family information, phone numbers, previous addresses and date of birth. It is critical to understand which data collection scenarios could result in the greatest negative impact, what forms of information sharing an individual can participate in will minimizing or avoid the risk of impact, and which scenarios must come with a level of risk acceptance. When evaluating the choices made on a daily basis, it is useful to note the types of impact that may result from unintended exposures of one's digital footprint. Some impacts include:

- **Identity theft** – Criminals who acquire digital records that include an individual's social security number may attempt to assume that person's identity with the intent to make transactions or purchases. Combating identity theft can lead to lost time and money.

- **Employment** – Information posted to social media accounts like Facebook, Twitter, and LinkedIn are increasingly being used to screen new applicants and have been used to dismiss employees from their current jobs.[10]

- **Court Cases** – Lawyers may use information found in an individual's digital footprint to discredit them based on what may be argued as evidence of their character.[11] Information or behavior captured today may be used years later.

- **Education** – Depending on an institution's policies, information in a student's digital footprint (most often from social media) may impact their education status including suspension, expulsion or loss of scholarship opportunities.[12]

- **Financial Theft or Fraud** – Credit and debit card information may be stolen from retailer database or payment system and used for fraudulent purchases. Cyber criminals may also use other tactics such as phishing, where a malicious actor uses bank themed e-mails to trick the end user into revealing their bank account user name and password.

- **Phishing** – Individuals supply their e-mail addresses when making a purchase, signing up for coupons, applying for jobs or loans and establishing a social media or payment account among other activities. These activities place this contact information in a multitude of databases. Whether malicious actors breach these databases or locate your e-mail address on a publicly available business or personal website, it can be used for spam, phishing, or spearphishing campaigns; all of which can result in theft of other credentials as well as malware infections.

Risk can be defined by threats, vulnerabilities, likelihood a threat will occur, and impact should the threat occur. Consumers may then address the impact using the concepts of mitigation, transfer, avoidance and acceptance.[13] Almost any activity that contributes to the creation of a digital footprint has associated risks. In every case possible, consumers may want to take a more active role in determining if the benefit of taking the risk outweighs the potential impact. Some may determine the convenience of receiving coupons while in a store, or using a particular mobile app outweighs the loss of a certain level of privacy. Others may decide the time and effort to browse the internet privately and increase the security of their accounts through complex passwords and multiple factor authentications outweigh the convenience of speed.

Choosing to entirely avoid risk associated with a digital footprint most often means not creating one (e.g. refraining from starting social media or online pay accounts, purchasing goods and services with cash, never giving your contact information, including your e-mail, to anyone). Therefore, individuals may want to take a more realistic approach to protect their data. Some proactive steps include:

- **Browser Privacy and Security Settings and Ad-ons**: These settings and ad-ons offer options to control how the browser handles history, what sites can send you cookies and remove the cookies sites have sent you, browse privately and prevent websites from tracking your behavior.[14,15,16,17,18] Some browsers also offer security and privacy add-ons with options for Firefox[19], Chrome[20], and IE[21] for things like Ghostery[22], Adblock Plus[23], and Web of Trust.[24,25]

- **Cookies***:* Clear your cookies; Most browsers offer step by step assistance for users that wish to adjust their cookie and site data permissions.[26,27,28,29]

- **Software***:* Always update anti-virus software and install patches when available to all software. Update security patches and hotfixes are issued to address or resolve known vulnerabilities or performance issues. [30]

- **Multi-factor Authentication***:* Always opt-in to multi-factor authentication when offered. Many accounts either offer multi-factor authentication or require it. A user name and password combination is considered single factor authentication. Multiple factor authentication requires two or three of the following categories: something you know, something you are and something you have.[31] Some examples include Facebook's use of mobile notifications. If a user chooses the option, Facebook will restrict a user from logging in to an unknown device until the user enters a

onetime security code/number that was sent to the registered user via text.[32] Other examples include Google similar account recognition service,[33] Microsoft Office 365 log in requirements,[34] and the use of U.S. Federal Government personal identity verification (PIV) cards[35] or Department of Defense common access cards (CAC) to access computer systems.[36]

- **Location-based services***:* Location based services include but are not limited to geo-tagging pictures, generating coupons based on stores a consumer is near or in, locating businesses or services nearby and generating directions based on current location[37] Some services continue to collect location information and store indefinitely even when you're not using the service. Deselecting the location based services option while not in use is best practice for consumers interested in the highest level of privacy.

- **Verify Security Level of Sites Requesting Data Entry:** Generally pages that require a user to log in or enter sensitive information like payment card numbers will be displayed as "https" indicating the use of Secure Socket Layer (SSL) for data encryption. Be wary of login pages whose URL are displayed as "http".[38]

- **Consider Full Disk Encryption:** on all laptops to prevent data theft in the event the device is lost or stolen.[39]

- **Read the privacy policies and guidelines**: as they sometimes change and often inform individuals if and how their personal information may be shared with other parties.

- **Use complex passwords**: that are not based on personal information, cannot be easily guessed, and cannot be found in any dictionary. Also, to avoid being exploited under multiple accounts use different passwords on different systems and accounts.[40]

- **Routinely change debit card PINs**: Contact or visit your financial institutions website to learn more about available fraud liability protection programs for debit and credit card accounts. Some institutions offer debit card protections similar to or the same as credit card protections.

- **Accessing Public Wi-Fi:** Whether via cell phone, tablet or laptop, consumers should practice caution when accessing public Wi-Fi. When possible, VPN into the hotspot to encrypt your communications.[41] When not possible it's best practice to avoid online shopping or other activities that require payment card data or log in credentials.[42]

- **Home Wi-Fi Settings:** When an internet service provider (ISP) technician installs the hardware necessary for home internet access, they often explain the use of the modem and whether the modem is also a Wi-Fi router or if the consumer must purchase one. In any event, either the ISP associate or the user documentation with the router may also aide the consumer in the following:[43]

    - **Change default/administrator passwords:** used during setup; these default device credentials can often be located online and therefore used to compromise commercial devices.

    - **Encrypt the data on the network:** using WEP (wired equivalent privacy) or WPA (Wi-Fi protected access). WPA is more secure than WEP and should be used if available.

    - **Change and/or do not broadcast the network's SSID:** This may make it more difficult for unauthorized users to easily access the network.

- **Install a firewall:** Installing a host based firewall directly onto wireless devices add an extra layer of security.

- **Mobile Devices:** It is best practice to secure mobile devices via many of the same methods that are suggested for desktop or laptop computer security. Some best practices include:

  - **Device Privacy Settings:** Consider using the privacy settings available on smart phones or other mobile devices.

  - **Lock**: Take advantage of the lock feature on the device (common examples include: password, PIN, fingerprint recognition or sequence).

  - **AV Software**: Install anti-virus software; there are multiple free and paid versions available for all devices and operating systems. Most companies that offer antivirus solutions for personal computers also offer them for mobile devices. The following graph lists the top antivirus vendors according to independent software management and security technologies provider OPSWAT. Only antivirus products with real time protection (RTP) enabled are included in this comparison.[44]

Antivirus Vendor	Market Share	Mobile Security Information Provided by the Vendor
Microsoft	25.8%	http://www.microsoft.com/security/online-privacy/mobile-phone-safety.aspx
Avast	23.6%	http://www.avast.com/free-mobile-security
AVG	9.1%	http://www.avg.com/us-en/for-mobile
Symantec	8.4%	http://www.symantec.com/mobile-security
ESET	7.1%	http://www.eset.com/us/home/products/mobile-security-android/
Avira	6.6%	http://www.avira.com/en/avira-android-security
Kaspersky	5.8%	http://www.kaspersky.com/android-security
McAfee	3.1%	http://www.mcafee.com/us/campaigns/mobile-security/downloads.html
Bitdefender	2.1%	http://www.bitdefender.com/solutions/mobile-security-android html
Other	8.4%	

Figure 2: Top Mobile Anti-Virus Vendors

  - **Mobile Applications:** Download software and applications (apps) only from trusted sources like Google Play or the Apple App Store.

- **Social Media Precautions:** it's important to consider all of the privacy and security options available on social media accounts. Though some consumers may not believe they have a need for increased security or privacy, unforeseen events in the future may change that perception. Some general recommendations include:

  - Adjust account privacy settings.[45]
  - Disable all sharing options on accounts then enable one by one.[46]
  - Limit what is posted and whom posted information is shared with; even if e-mail addressed are made publicly available, it could increase the amount of spam or phishing e-mails received.

- **Monitor credit report:** Under federal law, consumers are also entitled to one free copy of their credit report every twelve months.[47] Monitoring credit reports may aid in identifying attempts at identity theft or fraudulent charges.

- **Mitigating Impact**: If consumers have a reason to believe their credit or debit card information has been compromised, several cautionary steps to protect funds and prevent identity theft include:

    - Changing online passwords and PINs used at ATMs and point of sale (POS) systems
    - Requesting a replacement card
    - Monitoring account activity closely
    - Placing a security freeze on all three national credit reports (Equifax[48], Experian[49] and TransUnion[50]). A freeze will block access to your credit file by lenders you do not already do business with.
    - Consumers may also contact the Federal Trade Commission (FTC)[51] at (877) 438-4338 or law enforcement to report incidents of identity theft.

Mitigating Risk and Impact: Point of Sale Transactions

Choosing to be a proactive consumer may aide in the mitigation of risk or impact. However it is a 'whole of Nation' approach that will provide us the opportunity to accept reasonable risk while still allowing the flow of digital goods, transactions, and online interactions to occur in a safe and secure manner.[52]

Digital transactions, transference, and data storage to include those that occur at brick and mortar establishments as well as online account for a large part of an individual's digital footprint. The U.S. retail industry showed an overall increase of about 2-3% in 2013 compared to 2012 with non-store retailers being up nearly 7%.[53] A 2013 United Parcel Service (UPS) study of online shopping trends polled 3,000 consumers and noted that everyone polled would make an average of two online purchases every three months.[54] Market researchers concluded that currently, the online retail industry in the U.S. generates around $300 billion (USD) and by 2017 that number could increase to nearly half of a trillion dollars.[55] As retail consumption rates steadily rise, it is important that consumers are aware of how a simple act of buying groceries at the grocery store can add to their overall digital footprint and the risks associated with that.

Both the passive and active components of one's digital footprint are significantly impacted by online debit and credit card transactions and POS systems at brick and mortar locations. Current POS systems ingest "swiped" card data, transfer funds from financial institutions, and then store that card data on POS backend servers. Current credit and debit card statistics in the U.S. reveal that as of late 2013, there were a little over 390 million credit card accounts and roughly 570 million MasterCard and Visa debit cards.[56] The same trending suggests that in 2012 there were over 26 billion credit card transactions and 47 billion debit card transactions, which represents increases of 27% and 70%, respectively, since 2003.[57] In fact, about 67% of all transactions from consumers and businesses in 2012 were completed using a credit or debit card.[58]

Magnetic Strip Technology

The predominate technology used for credit and debit card payment in the U.S. is the magnetic strip. This technology dates back to the 1970's[59] when American Express, American Airlines, and IBM initiated the magnetic strip card technology into employee identification cards and some payment cards. The magnetic strip is similar to the tape used in video cassette tapes in that it can be embossed with specific data, which is referred to as Track 1, 2, and 3 data.[60] Some of the stored data consists of the 16-digit card number, 3-digit security code (CVV), the expiration date, and the card holder's full name. Typically, Track-2 data is the information that is captured during a transaction at a POS system. The inherent security risk with magnetic strip cards is that they are easy to reproduce and all of the information a criminal would need to create a fake card is physically located on the card itself. In addition, as evident by recent large scale retail POS system breaches[61,62], securing customer transaction data is not always a simple task. Despite following best practices and employing reasonable security measures, cyber

criminals continue to evolve their attack tactics therefore creating a constant need for defensive security actions to change as well.

Figure 3: This magnetic strip card making kit retails for about $150 online and can be run on a standard computer.

Chip Technology

One measure that has been implemented on a variable global scale began its adoption around 2000. Banks in Europe and other developed countries began issuance of the "Europe, MasterCard and Visa" (EMV) credit and debit card, also referred to as chip technology.[63] EMV cards do not have a magnetic strip on the back, but rather rely on a microprocessor chip that encrypts information transferred to a merchant, such as the card number, with a different encryption for each new transaction.[64] This technology requires the consumer to remember and enter a multi-digit personal identification number (PIN) or supply a signature that was established with the bank upon receipt of the card. This type of system can also use a physical signature at the POS terminal to authorize a transaction in lieu of entering a PIN; this is referred to as chip-and-signature. It's important to note that in addition to PIN or signature, a method is also available for 'no cardholder verification method'. This is used for unattended devices where transaction amounts are typically low, such as purchases at a fast food restaurant or a convenience store.[65]

The PIN and signature method may seem generally the same as the current magnetic strip technology, but chip technology uses a symmetric key technology, which generates dynamic data that makes each EMV transaction unique. Each unique encrypted transaction prevents a criminal from stealing transaction data from a database server or during transit as well as attempting to use the stolen data to create a fake card. The Smart Card Alliance offers multiple resources to aide in understanding static versus dynamic data authentication, the difference between online and offline options for EMV transactions and the chain of trust present in both.[66] The unique transaction data, in addition to the actual chip technology are the added layers of security that prevent fraudulent 'card present' purchases (i.e. swiping a card on a POS system in a brick and mortar locations) and would likely decrease an individual's footprint as a result.

Figure 4: Chip-and-PIN card example.

Chip technology also offers additional security for online purchases, but currently this added layer requires a compliant peripheral card reader attached to the computer being used to make the purchase. The consumer would insert the EMV card into the card reader, enter their PIN, and await the display of a one-time password which would be used to validate the consumer's identity. MasterCard Chip Authentication Program (CAP)[67] and Visa Dynamic Passcode Authentication (DPA)[68] support this form of authentication, which has reportedly been adopted by 30 million European users.[69] Similar chip based card technology is currently in use in the U.S. Federal Government PIV card and the Department Of Defense CAC.

The adoption of and transitioning to EMV card technology will undoubtedly result in increased costs bore by card issuers, which will eventually increase costs to merchants and consumers.[70] According to some sources, traditional magnetic strip cards may cost approximately 20 cents to create whereas EMV cards may cost up to $10 per card.[71] Depending on one's statistics, the argument is often made that the cost to

increase this level of security outweighs the annual cost (both quantitative and qualitative) incurred from fraud in the U.S.[72]

U.S. banks and card vendors have issued a road map for the U.S. market to adopt the EMV infrastructure by October 2015. Carolyn Balfany, the head of MasterCard's U.S. product delivery group, recently stated to the Wall Street Journal that as new technology is implemented, there could be a potential shift in liability after the October 2015 deadline.[73] Balfany indicated that in the event of fraudulent activity, whichever entity held the lesser technology could be the liable party (card issuer or merchant); however, this would require some form of official legislation. Balfany also goes on to suggest that other countries were more willing to switch to EMV technology sooner than the U.S. because fraud rates were much higher in many of those countries compared to the U.S. Interestingly enough, over 50% of the world's current fraud is committed against the U.S., which could be directly correlated to other countries instituting the EMV technology sooner.[74]

Near Field Communication

Another relatively new payment system is the Near Field Communication (NFC) payment system, which relies on proximity and radio frequency communication exchanges to transmit data (e.g. a payment). Unlike using a credit card, NFC transactions simply require holding a device such as a smart phone up to an NFC reader. The radio frequency exchange completes the rest including: generating the transaction, acquiring the customer's account/payment information, and obtaining the authorization to finalize the transaction. There are NFC enabled payment systems that use both cards as well as applications on mobile devices. The following are examples of each:

- Visa PayWave[75]
- MasterCard PayPass[76]
- Google Wallet[77]

Figure 5: Near Field Communication Device

Options to Consider

In an effort to mitigate both risk and impact associated with digital payment transactions, it's important that defensive measures continue to evolve. Though full scale adoption in the U.S. requires time and money on the behalf of all stakeholders involved in the creation and security of an individual's digital footprint, several options or combination of options to consider are as follows:

- Additional security could be added to online transactions via two factor authentication (2FA) methods. For example, a 'one time PIN' could be generated for each online purchase or transaction. When establishing an account with the card issuer, the consumer would need to select a delivery method of e-mail or text message. When the consumer attempts to make an online purchase, a one time PIN would be delivered to the preferred medium, the consumer would then retrieve the PIN then enter it into a field on the purchase screen to complete the transaction. This requires the consumer to have the card information (number, expiration and CVV) as well as access to the mail account or cell phone receiving the text message. Similar 2FA mechanisms are already in use when logging into many personal e-mail, bank, and other accounts globally.[78]

- Geo-location and IP address verification can be used by financial institutions during an online transaction to verify a previously linked or "trusted" IP address or physical address.[79] Before a

transaction is completed, the IP address or geo-location of the purchase's origination must be verified. Transactions originating from an IP address or geo-location not linked or "trusted" with the account are flagged as suspicious and the customer is contacted. Some account owners offer similar device-IP recognition options; users may recognize this feature if when logging in from a different device than what is commonly used, a message stating the device is not recognized will be displayed, subsequently requiring additional information (e.g. answers to security questions or the entry of a one time code that is often sent via e-mail or text).

- Financial institutions could send a continuity check for every transaction that registers on a customer's account. If a transaction alert looks suspicious or if the account owner does not recognize the purchase as one they've made, consumers have the ability to immediately communicate with the institution that they believe the purchase to be unauthorized.[80] Consumers can also opt to receive text messages for every transaction and not just potentially suspicious transactions.

Unified Approach: Shared Risk - Shared Responsibility

No single entity can ensure the security of an individual's footprint. Data privacy and security requires a unified approach. Following consumer and business security best practices is a baseline, but continual education is also useful.

Education and Awareness

Some of the many programs DHS promotes in an effort to increase cyber awareness and education are as follows:

- **STOP. THINK. CONNECT**.™ is the national cybersecurity education and awareness campaign. The message was created by an unprecedented coalition of private companies, nonprofits and government organizations.[81]

- **Data Privacy Day** held annually on January 28, encourages everyone to make protecting privacy and data a greater priority. DPD is an effort to empower and educate people to protect their privacy and control their digital footprint.[82]

- **National Cybersecurity Awareness Month** is October each year: it provides an opportunity to engage public and private sector stakeholders – especially the general public – to create a safe, secure, and resilient cyber environment. Everyone has to play a role in cybersecurity. Constantly evolving cyber threats require the engagement of the entire nation — from government and law enforcement to the private sector and most importantly, the public.[83]

- **National Initiative for Cybersecurity Education (NICE)** is a National campaign designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace.[84] Through NICE, DHS works with universities to attract top talent through competitive scholarship, fellowship, and internship programs.

Through these and similar programs, DHS promotes a safe and secure cyberspace. The more educational and information sharing opportunities that exist, the better we can defend ourselves as a whole Nation.

Conclusion

As innovation continues to change the world around us, expanding our digital footprint in sometimes more complex manners than we may realize, it is important for the shared risk to be approached by a whole Nation to share the responsibility of reducing the risk and potential impact involved. While protecting privacy, civil liberties and civil rights, a continual evolution and employment of new defensive

technologies and methodologies must always be complimented with continual progress in consumer awareness and best practice and private-public information sharing and incident response activities. We are all stakeholders in a secure cyberspace; DHS and the NCCIC encourage cyber awareness and education opportunities as well as information sharing to combat the evolving cyber threat. Please contact the NCCIC via or (888) 282-0870 for any questions regarding this product, or to learn more about information sharing, education opportunities analysis and incident response activities provided by or associated with our organization.

Can I share this product?

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

References

[1] http://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you html?pagewanted=all&_r=0
[2] http://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps
[3] http://www.zdnet.com/1-7m-mobile-apps-analyzed-users-tracked-and-put-at-risk-and-its-unjustified-7000006885/
[4] http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted%253Dall&_r=2&
[5] http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted%253Dall&_r=2&
[6] http://www.computerworld.com/s/article/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches
[7] http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/
[8] http://www.lib.odu.edu/genedinfolit/3searching/how_do_search_engines_work.html
[9] https://archive.org/web/
[10] http://online.wsj.com/news/articles/SB10000872396390443759504577631410093879278
[11] http://sites.ewu.edu/cmst496-stafford/2012/06/04/socially-convicted-social-media-in-law-enforcement-and-in-the-courts-part-2/
[12] http://www.huffingtonpost.com/2012/01/21/yuri-wright-don-bosco-football-tweets-michigan_n_1219749.html
[13] Elky, S. (2006, June 6). An Introduction to Information System Risk. Retrieved from: http://www.sans.org
[14] https://support.mozilla.org/en-US/kb/settings-privacy-browsing-history-do-not-track
[15] http://support.apple.com/kb/ht1677
[16] https://support.google.com/chrome/answer/114836?hl=en
[17] http://www.windowsphone.com/en-us/how-to/wp7/web/changing-privacy-and-other-browser-settings
[18] http://www.opera.com/help/tutorials/security/privacy/
[19] https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/
[20] http://www.chromeextensions.org/
[21] http://www.iegallery.com/PinnedSites
[22] https://www.ghostery.com/
[23] https://adblockplus.org/en/firefox
[24] https://www.mywot.com/
[25] http://howto.cnet.com/8301-11310_39-57583082-285/three-essential-security-add-ons-for-firefox-chrome-and-ie/
[26] https://support.google.com/chrome/answer/95647?hl=en
[27] http://windows.microsoft.com/en-us/internet-explorer/delete-manage-cookies#ie=ie-11
[28] http://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored
[29] http://support.apple.com/kb/ph11920
[30] http://technet.microsoft.com/en-us/library/cc750077.aspx
[31] http://www.pcmag.com/article2/0,2817,2428440,00.asp
[32] http://www.facebook.com/note.php?note_id=10150172618258920
[33] https://support.google.com/accounts/answer/180744?hl=en
[34] http://www.pcworld.com/article/2096560/microsoft-offers-multifactor-authentication-to-all-office-365-users.html
[35] http://csrc.nist.gov/groups/SNS/piv/index.html
[36] http://www.cac.mil/
[37] http://aclunc-tech.org/files/lbs-privacy-checkin.pdf
[38] https://www.globalsign.com/ssl-information-center/what-is-an-ssl-certificate.html
[39] http://www.nsa.gov/ia/_files/factsheets/best_practices_datasheets.pdf
[40] http://www.us-cert.gov/ncas/tips/ST04-002
[41] http://www.zdnet.com/10-security-best-practice-guidelines-for-consumers-7000012171/
[42] http://www.usatoday.com/story/tech/2013/07/01/free-wi-fi-risks/2480167/
[43] http://www.us-cert.gov/ncas/tips/ST05-003
[44] http://www.opswat.com/about/media/reports/antivirus-august-2013
[45] http://www.iacpsocialmedia.org/Resources/ToolsTutorials/ViewTutorial.aspx?termid=16&cmsid=5941
[46] http://www.sophos.com/en-us/security-news-trends/best-practices/facebook.aspx
[47] https://www.annualcreditreport.com/index.action
[48] https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

[49] http://www.experian.com/consumer/security_freeze.html
[50] https://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page
[51] http://www.consumer.ftc.gov/features/feature-0014-identity-theft
[52] http://www.dhs.gov/news/2014/02/05/written-testimony-nppd-house-energy-and-commerce-subcommittee-commerce-manufacturing
[53] http://www.census.gov/retail/marts/www/marts_current.pdf
[54] http://pressroom.ups.com/pressroom/staticfiles/pdf/fact_sheets/2013_PulseShopper_FINAL.pdf
[55] http://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/
[56] http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php
[57] http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php
[58] http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php
[59] http://www.creditcards.com/credit-card-news/history-credit-card-magnetic-stripe-1273.php
[60] http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit-card.htm
[61] http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html
[62] http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html
[63] http://www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf
[64] http://creditcardforum.com/blog/chip-and-pin-credit-cards-usa/
[65] http://www.tsys.com/acquiring/engage/white-papers/Cardholder-Verification-Method.cfm
[66] Smart Card Alliance. (September 2012). Card Payments Roadmap in the United States: How Will EMV Impact Future Payments Infrastructure? Retrieved from: http://www.smartcardalliance.org/pages/publications-emv-faq#Cardholderverification
[67] https://www.mastercardconnect.com/mol/molbe/public/login/ebusiness/smart_cards/one_smart_card/biz_opportunity/cap/index.jsp
[68] http://www.visaeurope.com/en/about_us/security.aspx
[69] http://www.smartcardalliance.org/articles/2011/05/05/smart-card-alliance-annual-conference-day-one-%E2%80%93-emv-and-the-united-states
[70] www.nl.capgemini.com/.../EMV_Compliance_in_the_U.S..pdf
[71] http://www.banktech.com/payments-cards/3-trends-in-emv-adoption-in-the-us/240165510
[72] http://www.diebold.com/Diebold%20Asset%20Library/dbd_emvcardfraudchipandpintechnology_whitepaper.pdf
[73] http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/
[74] http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/
[75] http://usa.visa.com/personal/security/card-technology/visa-paywave.jsp
[76] http://www.mastercard.com/contactless/index.html
[77] http://www.google.com/wallet/
[78] https://www.us-cert.gov/ncas/tips/ST05-012
[79] http://www.fraudlabs.com/fraudlabswhitepaperpg1.htm
[80] http://howsafeareyou.org/usaa-offers-text-as-a-way-of-preventing-credit-card-fraud/
[81] https://www.staysafeonline.org/stop-think-connect/about
[82] https://www.staysafeonline.org/data-privacy-day/about
[83] https://www.dhs.gov/national-cyber-security-awareness-month
[84] http://csrc.nist.gov/nice/