Identity Management in a Digital World

By Bryan Hjelm, VP of Product and Marketing at CSID

CSID.COM

CSID®

A part of Experian

INTRODUCTION

Prior to the Internet and the relocation of much of our personal data to the cloud, identity management was a simple matter of shredding papers with sensitive information, not sharing personal data with strangers in day-to-day life and not making a spectacle of oneself at work or in public. Today, identity management is a much more complex topic that includes relying on businesses to guard personal information, relying on those same businesses to not violate privacy by selling that information, and exercising a modicum of common sense when sharing personal information online. Identity management is also knowing what to do on occasions where a consumer or business fails at any of the above. There are serious consequences to a poorly managed identity that can range from financial problems to physical risks. These ramifications make the conversation around online identity management incredibly important.

In the ongoing discussion around online identity management, there are three main areas that individuals need to consider:

- **Transact:** the information we share with businesses and organizations online (and off)
- **Share:** the information we post to social networking sites and share with friends
- **Live:** the emerging frontier of the Internet of Things and devices that are always on, always connected, and always sharing.

TRANSACT

By 2017, 10.3 percent of total retail sales will be online purchases. This is compared to 5.2 percent of retail sales today. In 2013, 50 percent of US adults banked online.[1] Consumers are sharing more and more sensitive information online with entities that are tasked with collecting and protecting their information. This includes sites like Amazon and Zappos, where users make online purchases, as well as WellsFargo.com and Mint.com where users manage bank accounts, budgets, and bills. There are also mobile applications like Uber that are used to catch a ride and pay a driver. These are online entities that consumers are consciously providing personal information to, transacting with, and consenting to have them store the information. Consumers rely on these businesses and online entities to protect their personal information and keep it private. This has proven to be a difficult task.

RISK

The risks associated with online transactions are numerous. As last year's Target breach shows, businesses have difficulty keeping consumer credentials safe. Target's breach resulted in the loss of more than 40 million card numbers, including expiration dates, CVV codes and PIN numbers. Even those that made in-store purchases were not excluded from this breach. Personal information for more than 70 million customers – including names, mailing addresses, email addresses and phone numbers –- was also stolen.[2]

Consumers face identity and privacy risks even if they never make an online purchase or pay only in cash. In 2012, South Carolina's Department of Revenue suffered a severe data breach that resulted in the loss of 3.9 million tax returns and 387,000 credit and debit card numbers.[3] A 2011 breach in the Texas comptroller's office exposed 3.5 million Social Security Numbers and birth dates.[4] Consumers had very little control over the personal data shared with these two groups.

There is also a growing interest from identity thieves in credentials other than credit cards – credentials like email addresses and passwords. These credentials can provide access to valuable accounts like an Amazon or PayPal account. The value of these credentials underscores the risk of reusing passwords across multiple sites – something that sixty-one percent of consumers do. If one site is breached it is

very easy for a cyber criminal to check if that credential is used to log into a valuable site like Amazon.com or an online bank.

RISK MITIGATION

When it comes to online transactions there are three key actions a consumer can take to better manage their online identity and mitigate the negative impact of a business or organization losing their personal information. First and foremost, consumers should keep an eye on personal information with an identity protection service. Breaches like last year's Target breach often result in stolen personal information in addition to credit and debit card numbers – information that can be used for identity theft and other types of fraud. An identity protection service can alert users when personal information has been compromised. These services can also provide advance warning before the compromised information can be used for nefarious purposes and help with identity restoration in cases where it has already been used.

Consumers should also consider paying with credit cards when making in-store and online purchases. Credit card companies cannot hold users liable for fraudulent purchases made on a credit card. This makes it a lot easier and quicker to recoup losses from a fraudulent credit card charge than when using a debit card and recouping losses from a bank.

The final risk mitigation tactic is to use unique passwords for all online accounts. An email or password compromised from one business' data breach can open up vulnerabilities across a multitude of completely unrelated websites such as banking, financial, online retailers, and the like. Free software programs available in black market chatrooms, where stolen information is frequently bought and sold, let cyber criminals quickly test email and password combinations against high-value websites with the explicit goal of exposing other accounts to fraud and misuse.

SHARE

In the past five years, the amount of digital information created and shared globally has increased by 900 percent to two zettabytes. In more understandable terms, this is two *trillion* gigabytes.[5] Social media has played a huge role in this significant growth. Nearly 100 hours of video are uploaded to YouTube every single minute – a number that is more than 20 times what it was six years ago.[6] Facebook users are uploading 350 million photos each day.[7] The sheer amount information we share on sites like Facebook, Twitter, LinkedIn, Instagram and FourSquare has huge implications for online identity management and privacy.

There are also sites that consumers don't consent to – information aggregation sites like Spokeo that scan for and collect personal information from sources all over the Internet. These sites make public record files like real estate, county assessor, and directory assistance data available to anyone with an Internet connection.

RISK

The risks of sharing too much personal information on social sites can be severe. Individuals who are active on social media sites and share personal information online are at increased risk for identity theft. According to a 2013 Javelin Strategy & Research Identity Fraud Survey Report, 54 percent of social media users have been the target of an identity threat. The same research reports that accepting a friend request from a stranger can increase the likelihood of being a victim of fraud by 7.4 percent. Users who "checked in" using GPS have a 7.3 percent increase in fraud incidence rates.

There are also reputational risks. A teenager's online reputation can mean the difference between getting into a dream college or not. For an adult, it could be the key that unlocks a new business opportunity or

relationship. For job seekers, the importance of a good online reputation is magnified. According to a 2011 Reppler survey, 91 percent of hiring managers now look at social media when screening job applicants. A 2013 Jobvite survey found that 42 percent of companies have reconsidered job candidates based on the content of their social profiles, including Facebook, Twitter and Google+. Finally, there are actual physical risks associated with online sharing. When individuals post about an upcoming vacation on Facebook or check in to a location on FourSquare, they are basically broadcasting that they are not home. There is a website called PleaseRobMe.com that aggregates and streams location check-ins into a list titled "all those empty homes out there."

For teenagers the real-world risks of online sharing can be more severe. Cyber bullying is a growing threat for teenagers participating and sharing information on social networks. Seven out of 10 young people have been victims of cyber bullying and 37 percent of those experience it on a frequent basis.[8] These interactions are often carried into the real world in the form of bullying at school. What teens post online can also prove harmful to their parents. In February of 2014, a girl bragged about a settlement her father had reached with a former employer on Facebook. The father lost out on the $80,000 settlement because the daughter broke the confidentiality clause of the settlement.[9]

RISK MITIGATION

The emerging frontier in the identity management and privacy conversation is the Internet of Things (IoT) – a trend where more devices are connected, most of which are collecting and sending data. The growing number of devices being connected is mind-boggling. Cisco estimates that there will be 50 billion connected devices by 2020, up from 10 billion in 2013. This includes wearables like fitness trackers and connected watches, and home appliances like thermostats and refrigerators. Even the cars we drive will soon be collecting and sending data on our driving habits. To put this in perspective, the IoT will be larger than the smart phone, tablet and PC markets combined.[10]

The Internet of Things ushers in an era of data sharing ignorance. With social media sharing and ecommerce transactions, consumers have largely been aware of the types of data they are sharing and with whom. That is not the case with the Internet of Things. Much of the data being collected in the IoT is being collected passively, meaning that the consumer doesn't have to do anything for the device to collect and send data. The impact that this passive collection will have on identity management and privacy is not yet clear, but we are starting to the see what some of the implications might look like. In 2013 Google recently bought thermostat maker Nest for $3.2 billion. The company did not purchase Nest solely for its hardware, but rather for what the hardware can tell the company about its users, namely what people are doing when they are actively in front of their computers.[11]

LIVE

Consumers are starting to realize the importance of identity management and privacy when sharing information online. According to Javelin Research's 2014 Identity Fraud Report, 70 percent of Facebook users limit their profile visibility to only friends. Similarly, consumers are less likely to display common pieces of sensitive information on their social networking profiles. It is important for consumers to be aware of the potential ramifications of what they share online and what is publically available for others to see. It is also important to remember that when it comes to social networks, consumers are the product, not the customer. Facebook is valued at more than $100 billion not because of its platform or software, but because of the amount of data it has on all its users – data that is incredibly valuable to advertisers, a major source of Facebook's income.

In addition to general awareness, there are social media monitoring tools available and in development aiming to help individuals concerned about their own online reputation and privacy and that of their

children. These services alert users when sensitive information like date of birth or home address is posted or found online. These services will also assist with reputation management and alert a user when content is found on their social network profiles that may be compromising. This can include several different categories of potentially damaging content such as foul language, sexual content, and drug and alcohol references. Some services can even automatically suppress personal information on aggregation sites like Spokeo.

RISK

As we move further into the era of the Internet of Things, the identity management and privacy conversation gets a lot more interesting. These devices will have information on consumers that range from the normal – email addresses, home addresses, birthdates – to the more abstract like what TV shows we watch, how much we exercise, what hours we are typically at home or away and where we are. There are also privacy risks like unlawful surveillance (an extremely sensitive topic in the day and age of Edward Snowden and the NSA), active intrusion in private life, and data profiling.[12]

In January 2014, security firm Proofpoint uncovered a cyber attack that had more than 100,000 connected devices sending out spam emails. One of these devices was a refrigerator.[13] Granted, an Internet-connected fridge doesn't yet house much personal information about its user, but it does show the vulnerability of these newly connected devices. And there are "smart" devices that do collect sensitive information – pedometers, glucose meters and heart rate monitors collect medical information; and thermostats and TVs track when you are in the house and what you watch, respectively.

RISK MITIGATION

The best risk mitigation practice in the IoT era is awareness and education. It is important to be aware of the tradeoffs of convenience versus data capture, and understand what PII you're sharing with the world.

It is equally as important to read the fine print when it comes to connected devices to find out what data they collect and what the company can do with it. Using an identity protection service that can alert users when personal information has been compromised is also wise in a cyber landscape that is still being defined.

Identity management has never been easy, but it will clearly need to evolve to become even more comprehensive as technology becomes more and more integrated in our lives.

ABOUT CSID

CSID, a part of Experian, is a leading provider of global identity protection and fraud detection technologies for businesses, their employees, and consumers. With CSID's enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection services extend beyond credit monitoring to include a full suite of identity monitoring and fraud detection services; identity theft insurance provided under policies issued to CSID; full-service restoration services; and proactive data breach services.

www.csid.com

ADDITIONAL SOURCES

[1] 50% of U.S. Adults Bank Online, PewResearch Internet Project, 2013
[2] Data Breach FAQ, Target, 2014
[3] FAQ about the Dept. of Revenue hack attack, CarolinaLive.com, 2013
[4] Breach in Texas comptroller's office exposes 3.5 million Social Security numbers, birth dates, *The Dallas Morning News,* 2011
[5 & 6] Wow... We're Now Sharing 2 Zettabytes of Data Each Year Online, All Twitter, 2013
[7] Facebook Users Are Uploading 350 Million New Photos Each Day, *Business Insider,* 2013
[8] Cyberbullying Statistics: The Annual Cyberbullying Survey 2013, Ditch The Label, 2013
[9] Teen's Facebook brag costs dad $80,000 lawsuite settlement, *BBC,* 2014
[10] The "Internet of Things" Will Be Bigger Than The Smartphone, Tablet, And PC Markets Combined, Business Insider, 2014
[11] What Google Really Gets Out of Buying Nest for $3.2 Billion, *WIRED*, 2014
[12] Privacy Implications of the Internet of Things, Infosec Institute, 2014
[13] Fridge sends spam emails as attack hits smart gadgets, BBC, 2014