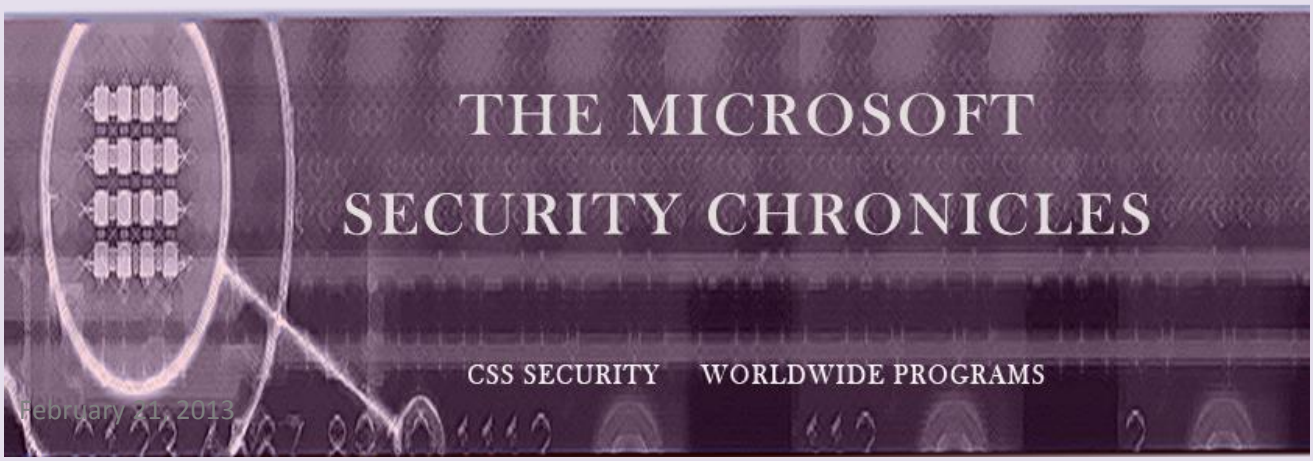


INSIDE THIS ISSUE

MICROSOFT RESOURCES

Microsoft Security Home

Microsoft Trustworthy Computing

SECURITY CALENDAR

March 2013

21 BSides Austin - Texas

24 APCERT - Brisbane

Microsoft Wants New Model for Online Privacy, Says Current One 'Can't Survive'

GeekWire

It's inevitable that companies will collect an array of data about people and their online activities. So rather than trying to prevent that data collection from happening, consumers should instead be given the ultimate control over how data is used.

Analysis:

In this article, Craig Mundie of Microsoft spoke to a group of reporters on the topic of online privacy. From his comments, "What we've been advocating for, and we're working on now around the world with data regulators and others, is to develop a new model, which is based on controlling usage, not controlling collection and retention of the data."

At the World Economic Forum, they provided a report (PDF) on Unlocking the Value of Personal Data: From Collection to Usage. In this report it cites that, "security and the overall stewardship of personal data remain central to the ecosystem." And more importantly, "who has data about you? And where is the data about you located? are impossible to answer today." Some key points:

April 2013

01 Financial Crytpography and Data Security 2013 - Okinawa

04 Microsoft Bulletin Advance Notification

08 Hack In The Box - Amsterdam

08 HackCon - Oslo

09 Microsoft Security Bulletin Release

11 Infiltrate 2013 - Miami

12 Hackito Ergo Sum - Paris

15 EuroSys 2013 - Prague

16 Source Boston

18 NotACon – Cleveland, Ohio

19 InfoSec Southwest 2013 – Austin, Texas

24 BSides London

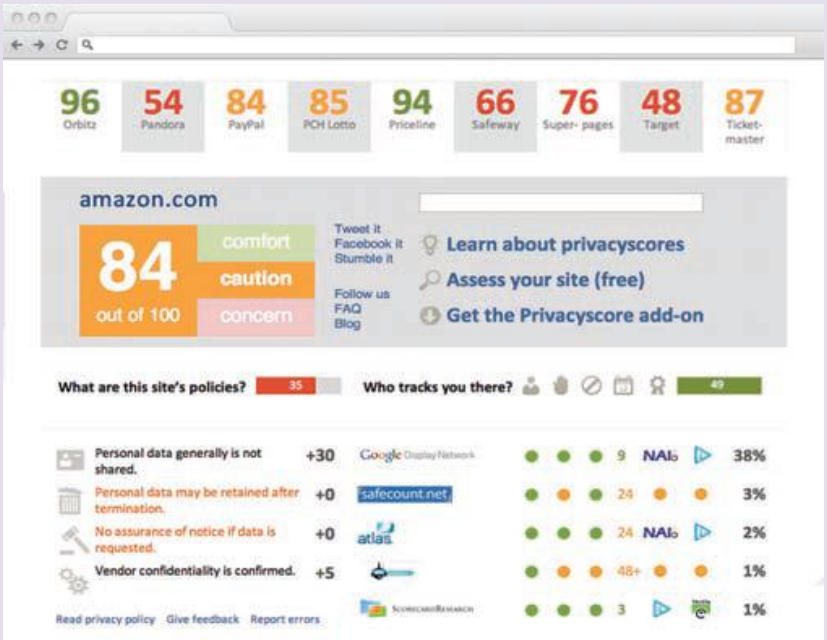
25 SyScan Singapore

26 THOTCON - Chicago

- *From transparency to understanding* — giving people the knowledge to understand the implications of allowing the usage of their data
- *From passive consent to engaged individuals* — people need to know where their data is going and how it is being used so they can make an informed choice
- *From black and white to shades of gray* — there is a need for flexibility to allow different approaches to using data in different situations

The biggest takeaway from this report (and Craig Mundie's talk) is the need for a new approach to data privacy – how it is handled, used, stored, etc. "One of the missing elements of the dialogue around personal data has been how to effectively engage the individual and give them a voice and tools to express choice and control over how data about them is used." The report mentions that several governments are working with the private sector to give individuals a locker to store their private information and share with who they want. There are also some great charts that show different tools to help people see how their personal data is being used (here is an example):

Privacyscore helps individuals understand how different websites use data



Source: www.privacyscore.com

WolframAlpha helps individuals visualize vast quantities of social data about them

Source: www.wolframalpha.com/facebook/

The issue of privacy has become not just about your personally identifiable information (PII) but it is about how companies are using your non-PII data to make predictions, sell you items, and advertise to you specifically. Is it ethical? One article believes that it is an ethical issue when sites gather privacy information and then share it. Web browsers are getting into the mix by limiting how much they track users. This makes advertisers worried about not being able to pop up those personalized ads. Microsoft already rolled out their Do-Not-Track feature in IE10. Europe is working on the privacy issue with the, "right to be forgotten."

Is information posted on the Internet really private? Some will say that it should be and others will say that you shouldn't expect it to be. There has been an on-going battle with Facebook about privacy. Every time we think our Facebook profile is locked down, they provide new settings that are open by default. Some pressing Internet privacy issues for 2012 were social networking, hacking, cookies, and malware. It seems like we have the same issues for 2013.

The biggest issue facing privacy is apathy. If users don't care that their information is being used for specific advertising purposes, what's the harm? "A lot of people think about privacy but don't really care until something happens to them personally," said Beth Givens, director of the Privacy Rights Clearinghouse. "It's like freedom. You don't appreciate it until it's gone. If you are a victim of identity theft, you experience a change of world view, you realize how little control you have over your world." The privacyrights.org site gives information about online privacy and how to use the Internet safely. It includes four main sections:

1) What Internet activities reveal my personal information
2) How do others get information about my online activity
3) Cloud computing
4) Resources

This is a great site to help sort out what it means to use social media, financial banking, and browsing the Internet.

With our children growing up with social media it is up to us to teach them that their privacy really does matter. Many kids are no longer interested in Facebook but are jumping onto Snapchat or Instagram. An Internet connection is all that is required to access these programs and an iPod Touch or Kindle Fire. Kids think that the Snapchat photos disappear after 10 seconds of being opened. Unfortunately, a screen capture can keep that photo forever. This article also pointed out that hackers are also jumping on these services to spread malicious hacker software and propagate scams.

Microsoft provides resources with regard to privacy. Included is information about setting up privacy controls in various Microsoft products and managing online reputations. A couple of videos can also be found on the site with regard to privacy in action and a personal data dashboard. There is also a great brochure that can be downloaded called protecting your privacy online (pdf).

Privacy is not something that is going away and is likely to get even more contentious. New "smart homes" that are Internet connected so that you can see everything going on with a smartphone or tablet will produce a lot of data that many would love to get their hands on. The privacy fears are real. It's one thing for advertisers to have access to data, but what about someone who is not only out to steal your identity but also your life.

Privacy is personal and many people guard it carefully. Unfortunately, too many others don't think about it until something bad happens. We all need to be aware of the risks and take precautions both on the Internet and in everyday life. It is best to be educated about privacy policies and take action to help protect children. Many of the technologies we take for granted also expose our privacy.

Everyone should know what privacy they are giving up any time they use a device or visit a webpage.

PA Health System Reports 144-Patient Data, Identity Theft

Health Security

In what's turned out to be a multi-layered case, 144 patients of Community Hospital in Chester and Crozer-Chester Medical Center in Upland, Pennsylvania [U.S.] had their names, dates of birth, and social security numbers stolen in an [U.S. Internal Revenue Service] IRS tax fraud sting from January 2008 to September 2011.

Analysis: Identity theft has topped the list of complaints filed in the U.S. to authorities according to the U. S. Federal Trade Commission (FTC). The FTC in February 2013 released a report called The Consumer Sentinel Network Data Book for January - December 2012 (PDF). The report listed identity theft as the largest category for 2012 U. S. consumer complaints (18 percent). Identity theft was listed as the largest category and largest growing category for 2012.

Report Takeaways

Identity Theft (2012) consisted of:

- Government Documents/Benefits Fraud 46%
- Credit Card Fraud 13%
- Phone or Utilities Fraud 10%
- Bank Fraud 6%
- Employment-Related Fraud 5%
- Loan Fraud 2%

➢ Complaints about government documents/benefits fraud increased 27 percentage points since calendar year 2010

- Tax or wage-related fraud accounted for the growth in this area, with 43.4% of identity theft victims reporting this problem in 2012.
- Employment-related fraud complaints, in contrast, have declined 6 percentage points since calendar year 2010.
- Florida is the state with the highest per capita rate of reported identity theft complaints, followed by Georgia and California.
- The age group most affected were younger adults 20-29 (21%), 30-39 (19%), 40-49 (18%) and 50-59 (17%). U. S. Retirees — 60 to 69 and 70 and over — were affected 11% and only 8%.

The Consumer Sentinel Network (CSN) or data contributors included all FTC complaints along with U.S. Better Business Bureau, police reports, state departments of justice and attorney general offices, Publisher's clearing house and the like. Exact organizations are listed in the report (Appendices A1 through A4 for complete list).

InfoSecurity reports, "[The year] 2012 saw a thirty-two percent increase over 2011 in terms of the raw number of instances, according to The Identity Theft Resource Center, a non-profit organization established to support victims of identity theft in resolving their cases."

The IRS has also seen an increase in resource allocation to identity theft. They reported an increase in identity theft investigations initiated of 898 in calendar year 2012 from 276 and 224 in calendar years 2011 and 2010, respectively.

According to the report, Florida is the state that had the most incidences of consumers being victimized by a large margin. In an effort to combat the existing identity theft, the U.S. Internal Revenue Service (IRS) has increased manpower in identity theft fraud. Many have been tried and convicted. One story included a Tampa, FL car dealer. This individual was sentenced to 15 years for fraud. Another story includes two Miami, Florida police officers being arrested for ID theft, and tax refund fraud. In the Miami Herald, Miami U.S. Attorney Wifredo Ferrer said, "the perpetrators of this type of [tax] fraud have been as diverse as the victims they prey upon. To date, we have prosecuted Social Security office employees, hospital employees, clinic workers, former NFL players, gang members, and violent criminals, to name a few. Today, we sadly add law enforcement to

The new FTC Chair Edith Ramirez has stated she is expecting to maintain privacy as a primary goal with a self-monitoring stewardship requiring evidence and research to dictate enforcement, "she also made it clear that she doesn't think the agency's authority to police unfairness gives it carte blanche on any privacy issue." The article also mentioned that the new chair was aware of and following discussions in Asia and Europe.

To assist consumers and attempt to thwart the upward trend, the FTC recently tweeted, "All the FTC's #idtheft materials were recently updated. Check them out: http://www.ftc.gov/idtheft #ChatSTC". The #ChatSTC hashtag stands for the STOP.THINK.CONNECT Twitter Chat series initiative.

The IRS has also documented identity theft enforcement efforts here and have information on tax frauds including how to recognize and avoid them. A website dedicated to tips for taxpayers and victims about identity theft and tax return is also available here. The U. S. Social Security website also has information on how they verify and protect identities. Finally, Microsoft has information on protecting individual privacy at http://microsoft.com/security. The burden of protection is clearly on the individual and enterprise as these public organizations lack agility to research and gather evidence to enforce laws quickly.