EMBRY-RIDDLE
Aeronautical University
SCHOLARLY COMMONS

College of Security and Intelligence | Honors - Prescott

Spring 2015

Social Media and Intelligence

Megan Levin
Embry-Riddle Aeronautical University, Levinm1@my.erau.edu

Follow this and additional works at: http://commons.erau.edu/pr-honors-csi

Part of the Social Media Commons

Scholarly Commons Citation
Levin, M. (2015). Social Media and Intelligence. , (). Retrieved from http://commons.erau.edu/pr-honors-csi/1

This Presentation is brought to you for free and open access by the Honors - Prescott at Scholarly Commons. It has been accepted for inclusion in College of Security and Intelligence by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

Social Media and Intelligence

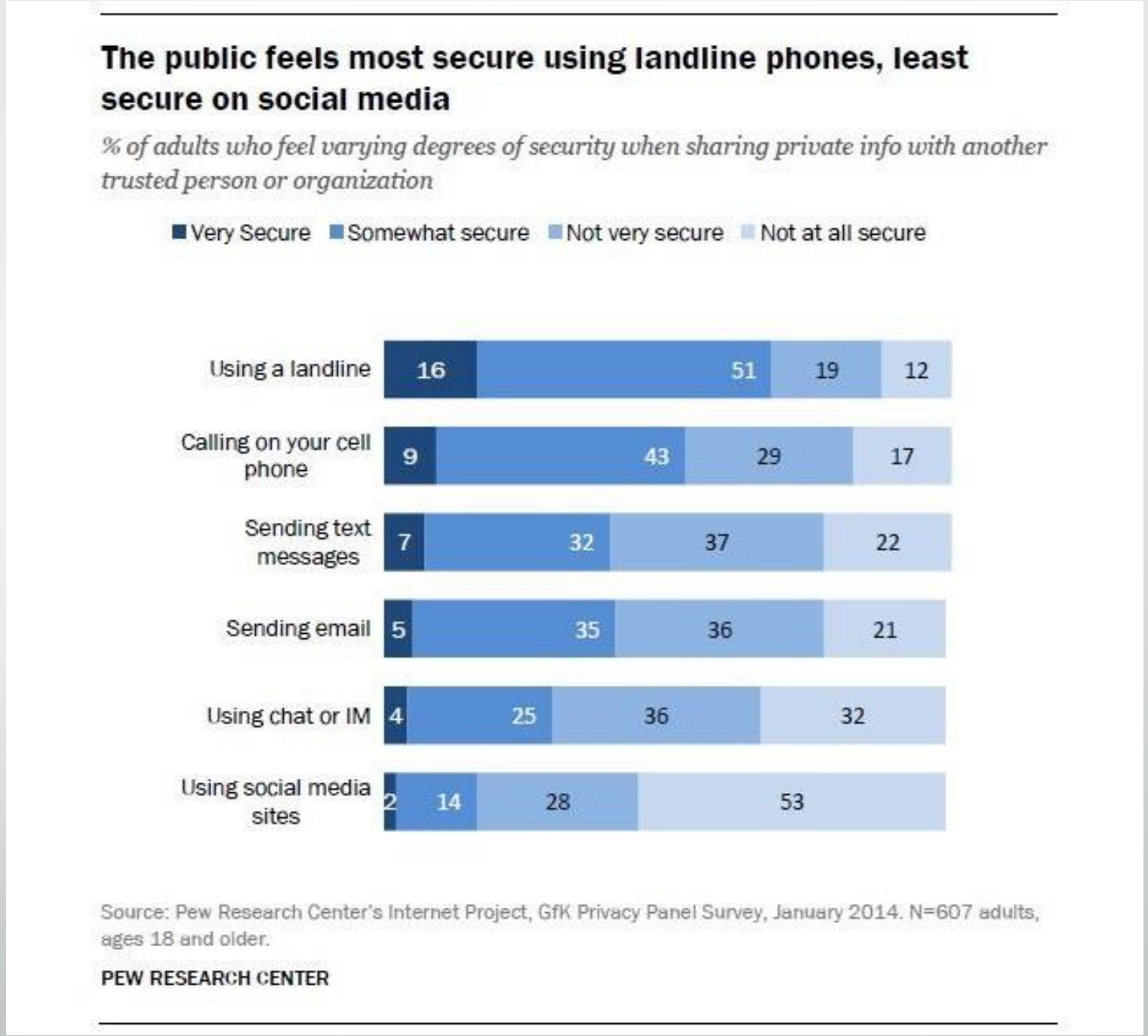
By: Megan Levin

Honors Directed Study Spring 2015

Overview

- Background
- Risks
- Harm
- Assistance
- Takeaway

- Over 66% of adults online in America are connected to one or more social media platforms.
- There are over 750 million Facebook members. This makes it the 3rd largest nation in the world.



Is privacy dead?

- "People have gotten comfortable not only sharing more information and different kinds, but more openly and with more people."

  -Mark Zuckerberg

- According to Mark Zuckerberg, the creator of Facebook, privacy is no longer a social norm.

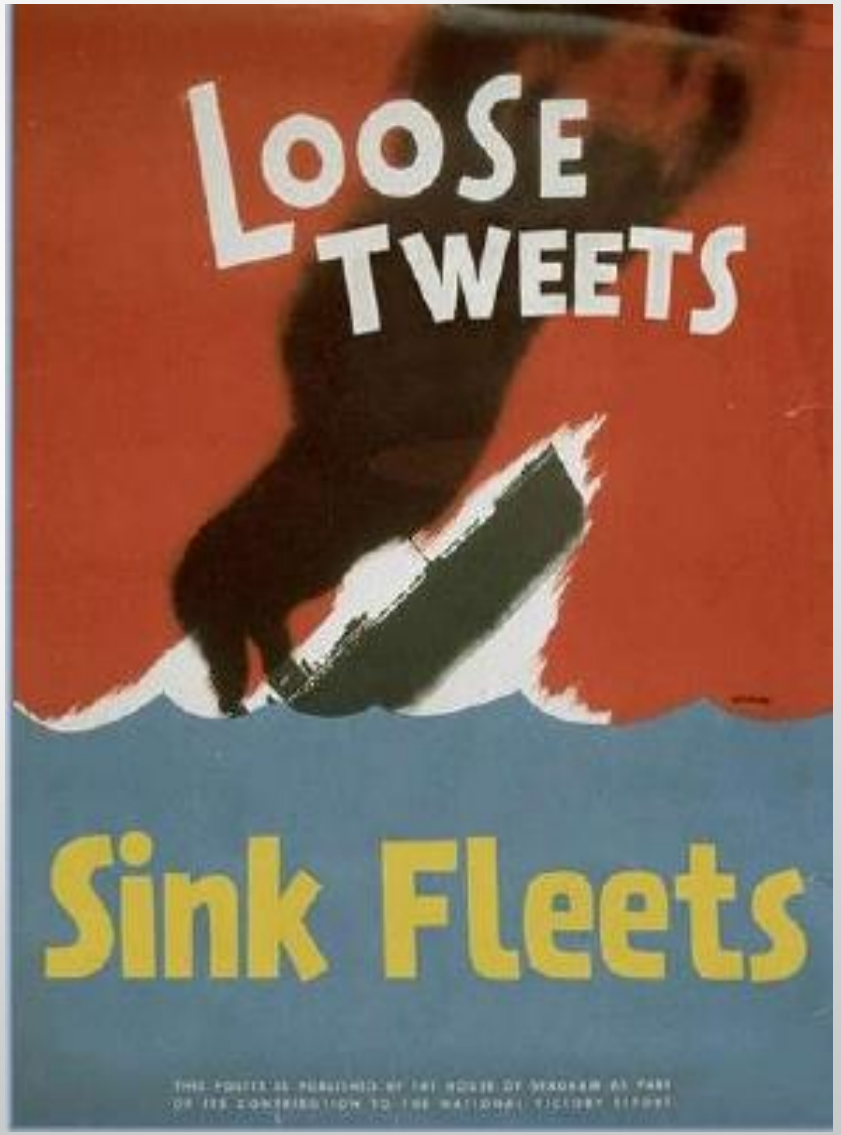
What Information is Out There? Who Can Gain Access?

- Information a user shares may include: photos and videos, age and gender, biographical information (employment, education, hometown, etc.), status updates, contacts, interests, geographic location.
- Viewers of this information can include: advertisers, third party software developers, identity thieves, other online criminals, debt collectors, applicant reviewers, etc.

What Can This Information Result in?

- Identity Theft/Impersonation
- Harassment
- Peer Pressure
- Lost Revenue or Income
- Loss of Employment
- Damaged Business or Personal Reputation
- Intellectual Property/Data Theft
- Malware/Virus Dissemination

OPSEC: activities designed to ensure the safety of intelligence, people, and assets.



The Taliban on Twitter

- The Taliban's Twitter account has followed the feeds of several U.S. military personnel since 2011.
- One of the individuals being followed, a U.S. Air Force logistics officer, had a link on his Twitter account to a personal blog.

ISIS and Twitter as "Yellow Pages"

- On 22 September 2014, an ISIS spokesman urged followers to attack citizens of the US, France, and other anti-ISIS countries.
- Tweets called on lone offenders in the US to use social media sites like Facebook, LinkedIn, and Twitter as modern "Yellow Pages" to find the addresses of service members.
- Followers were urged to "show up [at their homes] and slaughter them."

“Secret Trip”

- In 2009, Representative Peter Hoekstra, a member of the U.S. House Intelligence Committee, exposed his secret trip to Iraq.
- Representative Hoekstra tweeted his arrival in Baghdad, stating “Just landed in Baghdad. I believe it may be first time I've had bb [blackberry] service in Iraq. 11th trip here“.
- Not only did the trip become public knowledge, but Rep. Hoekstra continued to post his whereabouts as well as the entire party’s itinerary every few hours.

GPS Geotags

- When new U.S. army attack helicopters landed at an Iraqi base in 2007, soldiers uploaded smartphone photos to social media.

- The pictures contained GPS "geotags" which automatically embed latitude and longitude within photographs.

- Insurgents were able to locate and destroy four Apache helicopters with a mortar attack.

Terrorist Use of Social Media

- Facebook group pages and discussion forums are used to share operational and tactical information.
- Social media is used to export propaganda and extremist ideological messages.
- Forum threads created by groups dedicated to Hezbollah and other terrorist networks discuss OPSEC measures to maintain anonymity and how best to use social media.

Digital Propaganda

- An experimental unit of the State Department, the Center for Strategic Counterterrorism Communications (CSCC), counters al-Qaeda and other extremist groups by producing its own digital propaganda.
- @ThinkAgain_DOS is caustic and high tempo and actively looks for places to start fights.

Abu_Yusuf_1 Abu Yusuf

@ThinkAgain_DOS our dead are in paradise and yours are in hellfire. Either way we win either way yall lose. Simple as that

About 11 months ago via Mobile Web (M5) Favorite Retweet Reply

ThinkAgain_DOS Think AgainTurn Away

.@Abu_Yusuf_1 so what happens to your #alqaeda heroes when they butcher each other and their children? Heaven u say? http://t.co/PYvIQCJbK6

About 11 months ago via web Favorite Retweet Reply

Abu_Yusuf_1 Abu Yusuf

@ThinkAgain_DOS yep paradise. We hope Allah forgives their mistakes

About 11 months ago via Mobile Web (M5) Favorite Retweet Reply

ThinkAgain_DOS Think AgainTurn Away

@Abu_Yusuf_1 what kind of distorted ideology rewards murderers of children? Is this how #alqaeda defends Muslims by executing their children

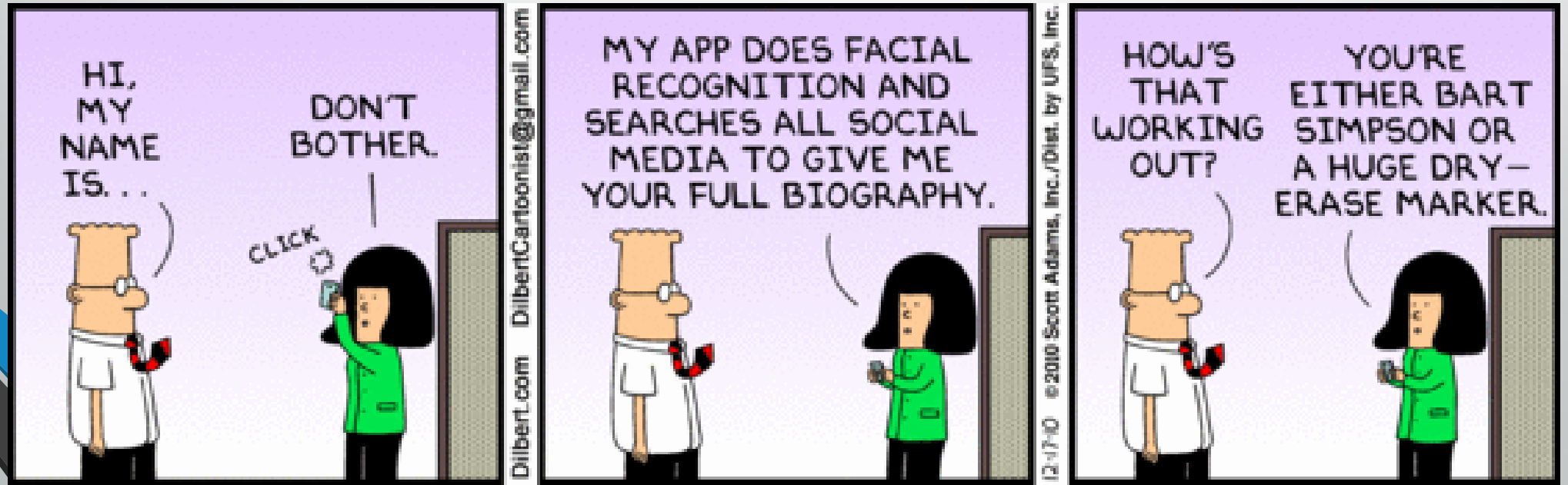
About 11 months ago via web Favorite Retweet Reply

SOCINT- "Social Media Intelligence"

- Minutes after Malaysia Airlines Flight 17 went down on 17 July 2014 in eastern Ukraine, killing all 298 on board, a DIA analyst sifting through social media got a "hit".

Social Media Facial Recognition

- The DIA has developed a classified facial recognition tool that scans social media. It was able to prove that Russian soldiers were moving into Crimea, Ukraine in 2014.



Takeaway

- Assume there is no privacy on social media.
- Maintain OPSEC.
- Extremists and terrorists have a significant presence on social media.
- Social media may be exploited as a tool for military and intelligence operations.
- Think of, and protect, your future career.

Questions?

Sources

- https://cdfai3ds.wordpress.com/2014/08/07/mark-collins-the-us-social-media-and-osint-mh-17-and-more/
- http://www.telegraph.co.uk/news/worldnews/al-qaeda/10829355/Tweeting-at-terrorists-inside-Americas-social-media-battle-with-online-jihad.html
- https://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/
- http://www.adweek.com/socialtimes/study-pew-public-perceptions-privacy/439321
- http://www.amazon.com/Know-Who-You-Are-What-ebook/dp/B004T4KXPU
- http://ncix.gov/issues/cyber/internet-social-networking-risks.pdf
- https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=0CFsQFjAJ&url=http%3A%2F%2Fwww.sdisac.com%2Fdocuments%2FSDICIWG_SocialNetworkingBestPractices.pptx&ei=mpfzVMzVH8rVoASz44CYCA&usg=AFQjCNGYSaulvKMOcfFqgnLJcssOgTnUvw&sig2=ifX3XJHCGCdkWdEsBlSOig&bvm=bv.87269000,d.cGU
- http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html

Sources (2)

- http://career-intelligence.com/social-media-negatively-affect-career/
- https://info.publicintelligence.net/ARTIC-HomelandThreatsISIL.pdf
- https://www.ctc.usma.edu/posts/the-taliban%E2%80%99s-conduct-of-intelligence-and-counterintelligence
- http://www.telegraph.co.uk/news/uknews/defence/10948490/Troops-leaked-confidential-data-on-Twitter-and-Facebook.html
- http://www.livescience.com/19114-military-social-media-geotags.html
- http://thelede.blogs.nytimes.com/2010/03/03/israeli-raid-canceled-after-facebook-leak/
- http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1092&context=ism
- http://www.infopackets.com/news/7328/facebook-scam-dupes-military-govt-officials
- http://wtvr.com/2015/03/13/the-dos-and-donts-of-being-a-cia-spy-in-the-facebook-age/