

WHAT HAPPENS IN VEGAS GOES ON YOUTUBE: USING SOCIAL NETWORKS SECURELY

Ben Rothke, CISSP CISM
Wyndham Worldwide Corp.

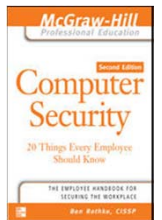
Session ID: STAR-107

Session Classification: Intermediate

RSACONFERENCE2012

About me...

- Ben Rothke, CISSP, CISM, CISA
- Manager - Information Security - Wyndham Worldwide Corp.
 - All content in this presentation reflect my views exclusively and **not** that of Wyndham Worldwide
- Author - *Computer Security: 20 Things Every Employee Should Know* (McGraw-Hill)
- Write the Security Reading Room blog
 - <https://365.rsaconference.com/blogs/securityreading>

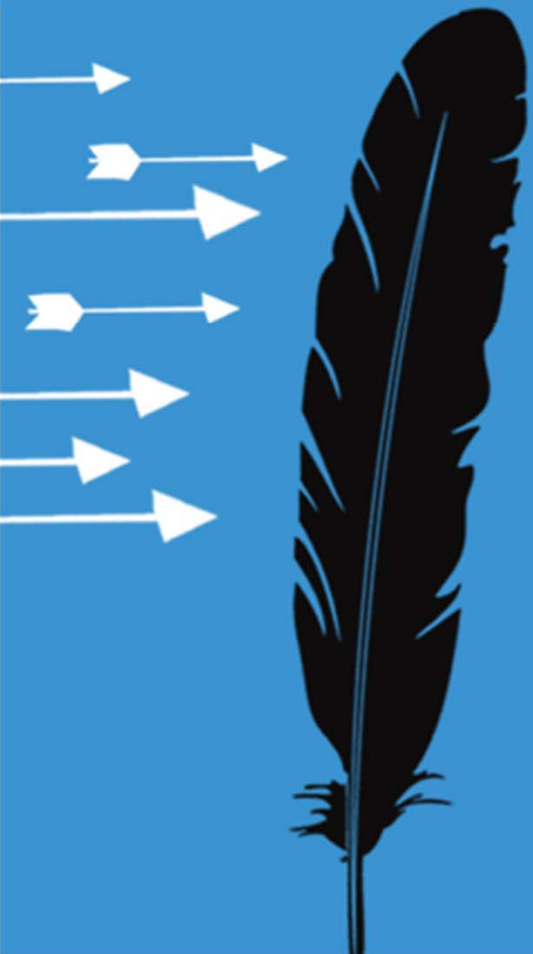


Agenda








- Overview of social networks
- Scary security risks associated with social networks
- Social network security strategies
- Conclusion / Recommendations / Q&A



Overview of social networks and the associated security and privacy



Social media explained

I need to eat	
I ate	
This is where I ate	
Why am I eating?	
Look at me eat!	
I'm good at eating	
Let's all eat together	



Social media is a infosec nightmare

[Home](#) > [Security](#) > [Cybercrime and Hacking](#)

News

Researcher finds major flaw in Facebook

The issue could allow hackers to send malicious software to people who aren't their friends

By Jeremy Kirk

October 27, 2011 12:18 PM ET

1 Comment



21



1

Social media protection

Sean Rintel

Published 9:21 AM, 7 Nov 2011
Sections [Social media](#)

Social Media Rewards

By Jose Granado & C
2011-02-02



Rodd Zolkos

Keeping employees off the social media black list

COMMENTARY: Risk, opportunity in social media

dark READING
Protect The Business Enable Access

Social Malice: One In 100 Tweets And One in 60 Facebook Posts Are Malicious

22 November 2011 Last updated at 05:25 ET

How much privacy can smartphone owners expect?

COMMENTS (244)

By Brian Wheeler
BBC News, Washington

Stealing Reality

Yaniv Altshuler,¹ Nadav Aharony,² Yuval Elovici,¹ Alex Pentland,² and Manuel Cebrian²

¹Deutsche Telekom Laboratories, Ben Gurion University, Beer Sheva 84105, Israel

²The Media Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

In this paper we discuss the threat of malware targeted at extracting information about the relationships in a real-world social network as well as characteristic information about the individuals in the network, which we dub *Stealing Reality*. We present Stealing Reality (SR), explain why it differs from traditional types of network attacks, and discuss why its impact is significantly more dangerous than that of other attacks. We also present our initial analysis and results regarding the form that an SR attack might take, with the goal of promoting the discussion of defending against such an attack, or even just detecting the fact that one has already occurred.

Summary

Maybe we should think twice about those Facebook, Twitter and Foursquare posts....

By Mary Mann | [Email the author](#) | 9:27am

Social Malice: One In 100 Tweets And One In 60 Facebook Posts Are

ACMA finds Facebook photos are not private

Brett Winterford | Dec 19, 2011 1:56 PM

Users offered no safety from Facebook-trawling.

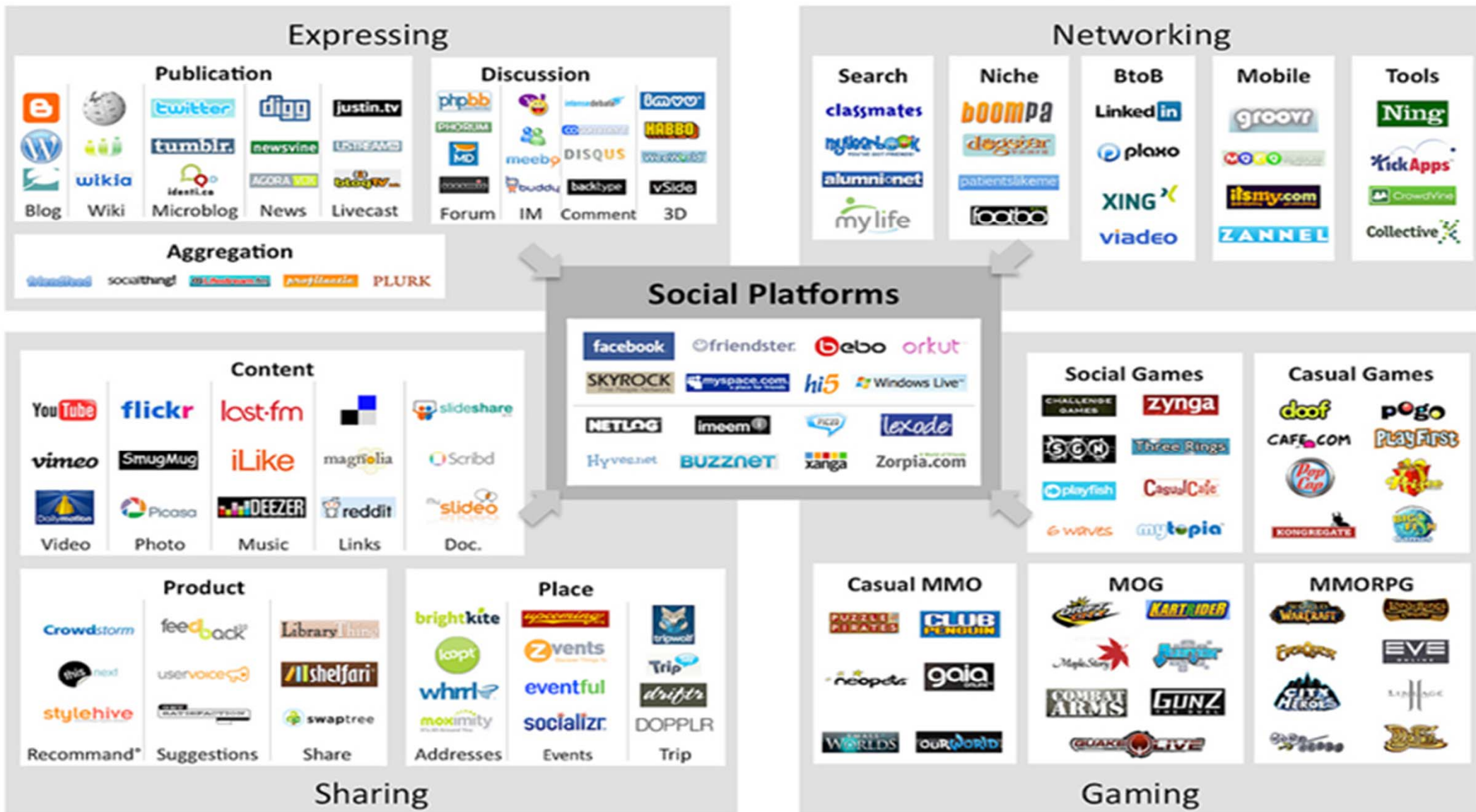


Services and social

businesses

id to a Home

Social media landscape



Social networking security reality

- People will share **huge amounts** of **highly confidential** personal & business information with people they **perceive** to be legitimate
- Numerous legitimate security risks with allowing **uncontrolled access** to social sites
- But...these risks can be mitigated via a comprehensive security strategy

**SOCIAL
MEDIA
HAS EMERGED
AS A MAJOR
NETWORK
SECURITY
THREAT**



Blocking is futile

- Not only is resistance futile – it's a negative business decision
- Prepare a social networking **strategy**
- Have a **realistic understanding** of the risks and benefits of social software
- Understand **unique challenges** and factor them into on when and how to proceed
- Business and information security goal is the **secure use and enablement of social media**



Does blocking increase risk of breaches?

- TELUS/Rotman Management School study:
 - negative correlation between organizations blocking access to social networking for security reasons and number of breaches experienced
 - when blocked, user may feel encouraged to use alternate method (smartphone/tablet) to access site
 - policy is actually forcing users to access non-trusted sites, using a technology that is not monitored or controlled by the enterprise security program

http://business.telus.com/en_CA/content/pdf/whyTELUS/Security_Thought_Leadership/TELUS_Rotman_2011_Results.pdf



Security game-changer

- Organizations and management are struggling
 - to understand and deal with the numerous security and privacy risks associated with social networks
- Traditional information security
 - firewalls and access control protected the perimeter. Social networks open up that perimeter
- Focus shift
 - from **infrastructure protection** to **data protection**



Social media security and privacy risks

Risk	Description	Security?	Type?
Malware	Infection of desktops, propagation of malware through staff or corporate profiles on social-media services.	Yes	Technology
Chain of providers	Mashups of applications within a social-media service enable the untraceable movement of data.	Yes	Technology
Interface weaknesses	Public application interfaces are not sufficiently secured, exposing users to cross-site scripting and other exploits.	Yes	Technology
Reputation damage	Degradation of personal and corporate reputations through posting of inappropriate content.	No	Content
Exposure of confidential information	<i>Loose lips sink ships</i> , breach of IP or other trade secrets, breach of copyright, public posting or downloading of private or sensitive personal information.	Yes	Content
Legal exposure	Legal liabilities resulting from posted content and online conversations or failure to meet a regulatory requirement to record and archive particular conversations.	Yes	Content
Revenue loss	For organizations in the information business, making content freely available may undercut fee-based information services	Yes	Content
Staff productivity	Workers failing to perform due to the distraction of social media	No	Behavior
Hierarchy subversion	Informal social networks erode authority of formal corporate hierarchy and defined work processes	No	Behavior
Social engineering	Phishing attacks, misrepresentation of identity and/or authority to obtain information illicitly or to stimulate damaging behaviors by staff.	Yes	Behavior
Identity fraud	Profiles and postings that are erroneously attributed to a staff member or corporate office.	Yes	Behavior

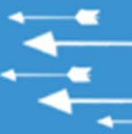


Social media security and privacy risks

- cross site scripting, cross site request forgery
- Twitter trending topic malware / spam
- LikeJacking
- phishing / spear phishing
- corporate espionage / business intelligence
- geolocation
 - Content-based Image Retrieval (CBIR)

- emerging technology that matches features, such as identifying aspects of a room (e.g. a painting) in very large databases, increasing the possibilities for locating users

<http://www.flickr.com/photos/narcissistic-indulgence/4472901190/>



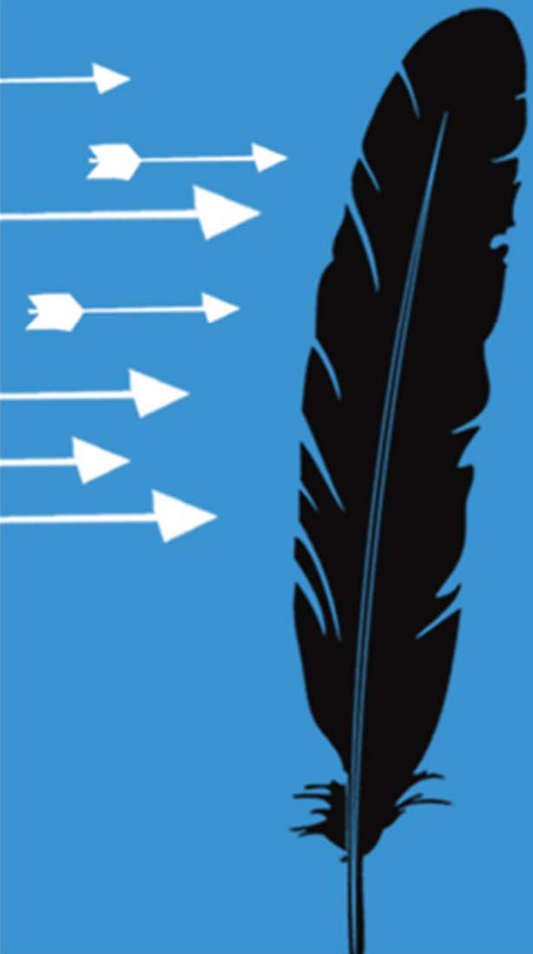
Aggregation



- Aggregation
 - process of collecting content from multiple social network services
 - consolidates multiple social networking profiles into one profile
- Long-term anonymity is nearly impossible
 - users leave traces, IP addresses, embedded links, IDs in files, photos, etc.
 - no matter how anonymous one tries to be, eventually, with enough traces, aggregation will catch up



Strategies and action items for enterprises to deal with the security and privacy risks of social networks



Social media waits for no one...

- Especially information security
- Be proactive
 - dedicated team to deal with social networks
 - ability to identify all issues around social networks
 - get involved and be engaged
- Be flexible
 - social networking is moving fast
 - too a rigid framework may be myopic
 - social media in 2013 will be quite different than 2012



Secure use of social media

1. Governance

- corporate social media strategy
- risk assessments
- realistic policies

2. Enablement

- awareness, education

3. Management

- monitoring



Governance - social media strategy

- Create a social media strategy based on **your** social media security goals
- Identify those who'll be online public face
- Draconian policies preventing the use of social media will most often not be effective
- Use a **balanced approach**
 - allow access
 - manage risk via technical controls, policies and employee training



Governance - risk assessment

- for each social network community
 - vulnerabilities associated with each community
- each social community has its own set of unique security and privacy concerns
- output will be used to create the social media policy and strategy
 - customized to your specific risk matrix
- balance risks vs. benefits
 - US Marines – some areas totally prohibited
 - Starbucks – totally embraced



Governance - data leakage

$$\sum_{i=1}^N p_i \dot{q}_i - L = \text{const}$$

- Social media physics - law of conservation of data
 - once confidential data is made public, it can never be made confidential again
 - once data is posted in a Web 2.0 world, it exists forever, somewhere
 - difficulty of complete account deletion
 - users wishing to delete accounts from social networks may find that it's almost impossible to remove secondary information linked to their profile, such as public comments



Governance - social media policy

- Social networking policy is a must
 - even if it prohibits everything, you still need a policy
- Employees will do stupid things
- Rational, sensible use of social media services
 - include photography and video
 - don't reference clients, customers, or partners without obtaining their express permission
- Social Media Policy Database
 - <http://socialmediagovernance.com/policies.php>



Governance - reputation management

- Goal is to build and protect a positive Internet-based reputation
- Risks to reputation are significant and growing with the increased use of social networks
- Create reputation management group with input from IT, legal, risk management, PR and marketing
- Coordinated approach
 - proactive / responsive



United Breaks Guitars

Visit www.UnitedBreaksGuitars.com for case studies and highlights from Dave's speaking tour. There is now a video response

by [sonsofmaxwell](#)
2 years ago
11,207,030 views



Taylor Guitars Responds to "United Breaks Guitars"

Bob Taylor lends his support to Dave Carroll and guitar players everywhere. Taylor has had an artist relationship with Dave for several years now ...

by [TaylorQualityGuitars](#) | 2 years ago | 583,447 views

Web [Show options...](#)

Verizon Store
VerizonWireless.com Save on VzW phones. Free overnight shipping with online orders!

Verizon - Store Locator
Verizon Store Locator. Shopping for Wireless Services? A complete listing of stores offering Verizon Wireless products can be found at Verizon Wireless. ...
[www22.verizon.com/Residential/.../sas/sas_StoreLocator.aspx](#) - [Cached](#) - [Similar](#) - [🔗](#) [🔗](#) [🔗](#)

Verizon | Residential & Business High Speed Internet/Broadband...
A leader in fiber optics, Verizon offers phone, Internet, TV, wireless and service bundles to residential, business, government and wholesale clients.
[www22.verizon.com/](#) - [Cached](#) - [Similar](#) - [🔗](#) [🔗](#) [🔗](#)

[Show more results from www22.verizon.com](#)

Store Locator - Verizon Wireless
Enter zip code or select the state where you want to shop for Verizon Wireless services.
[www.verizonwireless.com/b2c/storelocator/index.jsp](#) - [Cached](#) - [Similar](#) - [🔗](#) [🔗](#) [🔗](#)

New Cell Phones, CPO Cell Phones, Prepaid Cell Phones, Cell Phone...
Offers cell phones, PDAs, wireless mobile phone plans, data plans in the United States and parts of Mexico and Canada.
[My Verizon - Pay your bill online - Store Locator](#)
[www.verizonwireless.com/](#) - [Cached](#) - [Similar](#) - [🔗](#) [🔗](#) [🔗](#)

Woman Drags Child On Leash Through Verizon Store (VIDEO)
The headline doesn't lie: the following video really does show a woman dragging her child through a Verizon Wireless store on a leash, and at surprising ...
[www.huffingtonpost.com/.../woman-drags-child-on-leas_n_250033.html](#) - [Cached](#) - [Similar](#) - [🔗](#) [🔗](#) [🔗](#)

YouTube - Woman drags kid through Ve
This was taken of a mother dragging her kid thr dog. Apparently she has been arrested.
[www.youtube.com/watch?v=PtMRddAIHx0](#) - [Cs](#)

World's Worst Mom Drags Kid Through
What do you do if your child is acting difficult? I drag him through the mall.
[www.spike.com/video/worlds-worst-mom/32169](#)

Wtf. Mom Drags Kid Through Verizon :
Aug 3, 2009 ... "Woman Drags Child on Leash Wtf, abuse, bad parents, bad parenting. Videos consumerist.com/.../mom-drags-kid-through-ve

LiveLeak.com - Woman Drags Kid Thrc
Woman Drags Kid Through Verizon Store. CL arrested on child cruelty charge by Jeff Gable ..
[www.liveleak.com/view?i=a88_1249007894](#) - [Cs](#)

Mom Drags Kid Through Verizon Stor
Mom Drags Kid Through Verizon Store: This is it...
[www.buzzfeed.com/.../mom-drags-kid-through-](#)

Woman drags kid through Verizon Store

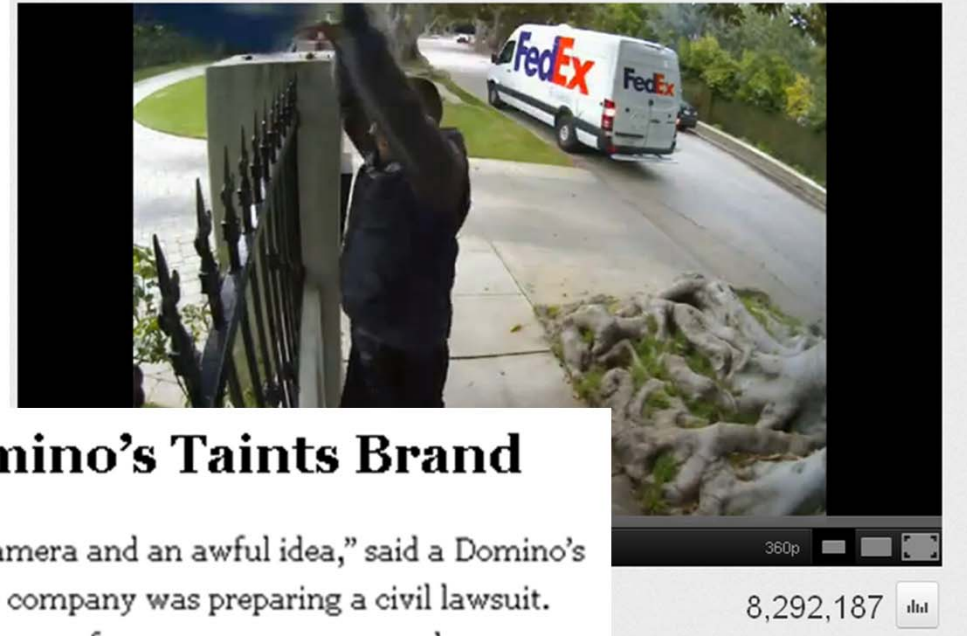
[TooMuchRock](#) 13 videos



0:00 / 0:17 240p **982,516**

FedEx Guy Throwing My Computer Monitor

[goobie55](#) 16 videos ▾



360p **8,292,187**

Video Prank at Domino's Taints Brand

"We got blindsided by two idiots with a video camera and an awful idea," said a Domino's spokesman, Tim McIntyre, who added that the company was preparing a civil lawsuit. "Even people who've been with us as loyal customers for 10, 15, 20 years, people are second-guessing their relationship with Domino's, and that's not fair."



Matthew Thornton, III
Senior VP, FedEx Express U.S. Operations
0:04 / 1:43 CC 360p **464,254**

Governance - reputation management

- Traditional PR and legal responses to an Internet-based negative reputation event can cause more damage than doing nothing
- establish, follow and update protocols can make social-media chaos less risky to enterprises
- Infosec coordinate activities with PR teams
 - expand monitoring and supplement monitoring with investigations and evidence collection processes



Enablement - awareness and education

- Social media is driven by social interactions
- Most significant risks are tied to the behavior of staff when they are using social software
- Don't shun social media for fear of bad end-user behavior
 - Anticipate it and formulate a multilevel approach to policies for effective governance
- 3 C's: clear, comprehensive, continuous



Awareness - *How to get fired in 3 tweets*

- Link social networking training to other related training
 - business ethics, standards of conduct, industry-specific regulations
- Let employees know they can lose their job
 - policy violation
 - managers and executives - special responsibility when blogging by virtue of their position
 - too much time on social network sites
 - perception that they are promoting themselves at the expense of the company



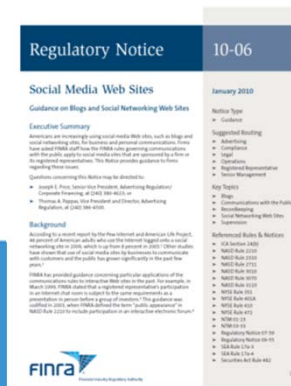
Awareness - curb your enthusiasm

- Awareness of addictive nature of social media
 - especially those with OCD/addictive personalities
- what is fun today is embarrassing tomorrow
- don't post comment that you don't want the **entire world** to see
- consider carefully which images, videos and information you publish
- set daily time limits on how much time they will spend



Awareness - regulatory

- Regulatory compliance must be considered
 - social networks present numerous scenarios which weren't foreseen when current legislation and data protection laws were created
 - regulatory framework governing social networks should be reviewed and, where necessary, revised
 - what specific laws/regulations/standards apply?
 - all breach notice laws are relevant
 - if customer or employee PII is posted, breach response plans would likely need to be followed and notices would need to be sent

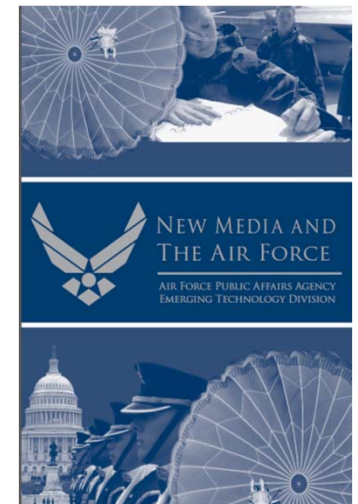
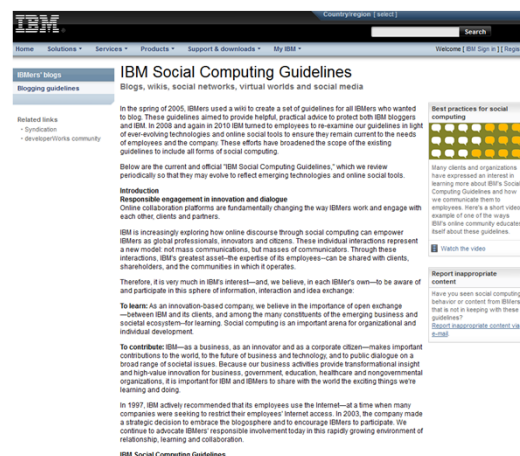
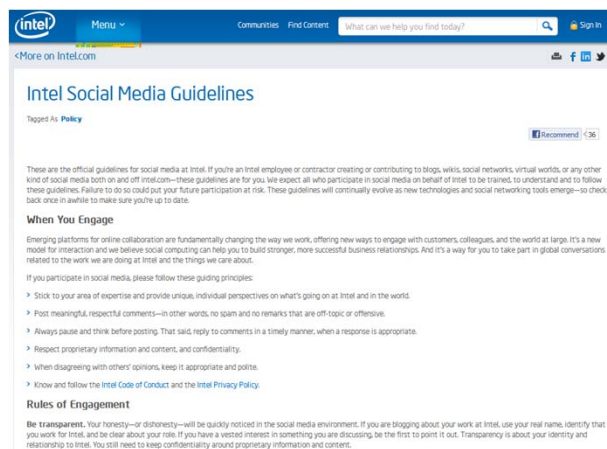


Awareness - corporate guidelines

- Without guidelines, breaches are inevitable

- Excellent sources:

- Intel Social Media Guidelines
- IBM Social Computing Guidelines
- United States Air Force – New media guidelines



Management - monitoring

- Maintain control over content company owns
 - monitor employee social networking participation
 - significant risk of loss of IP protection if not monitored
 - inappropriate use of enterprise content occurred?
 - notify employee - explain how their actions violated policy
 - control where and how corporate content is shared externally



Management - monitoring

- Monitor social media content for
 - inbound malware
 - potentially libelous comments that are sent externally, as well as trade secrets that might be referenced in social media posts, potential regulatory violations, breaches of ethical walls, etc.
 - sexually harassing, racist or other inappropriate content that might be sent internally.
 - employee posts on every social media site that might be used



Management - monitoring

- Gatorade's Social Media Command Center



- <http://mashable.com/2010/06/15/gatorade-social-media-mission-control/>





EU and social networks

- EU Directive on Data Protection 95/46/EC
- Data Protection Working Party Opinion 5/2009
 - EU countries take personal privacy **very seriously**
 - tagging of images with personal data without the consent of the subject of the image violates the user's right to informational self determination
 - blanket monitoring and logging is unacceptable in EU
 - many more privacy details need to be considered



Human resources must be involved

- Social networks open up a huge can of HR worms
- What are disciplinary actions for non-compliance?
- Can candidate's social network presence be a factor in hiring process?

Germany to ban spying on job applicants using social networks

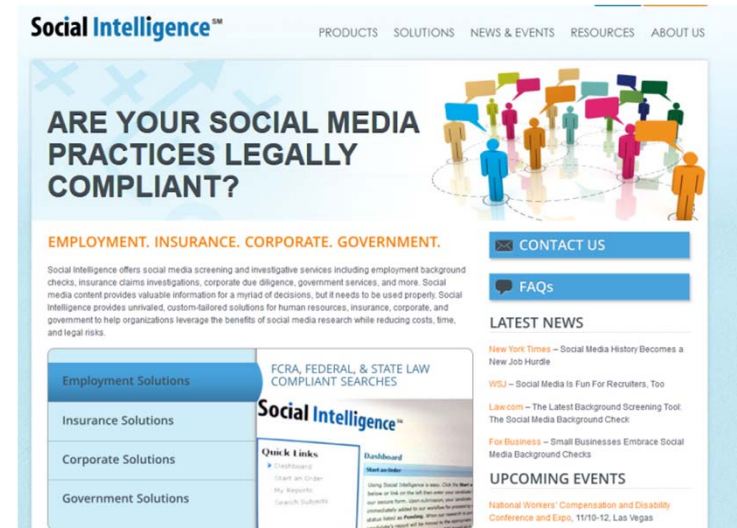
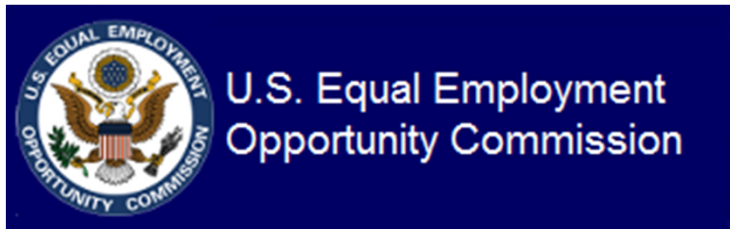
New Statesman

Published 26 August 2010



HR, FCRA and the EEOC

- via Facebook, you can know way too much about a candidate:
 - race, orientation, religion, politics, health, etc.
 - such information can be used to show bias
 - EEOC and expensive litigation



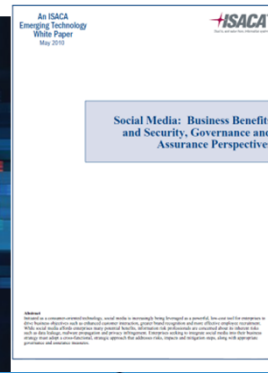
Social media hardware/software tools

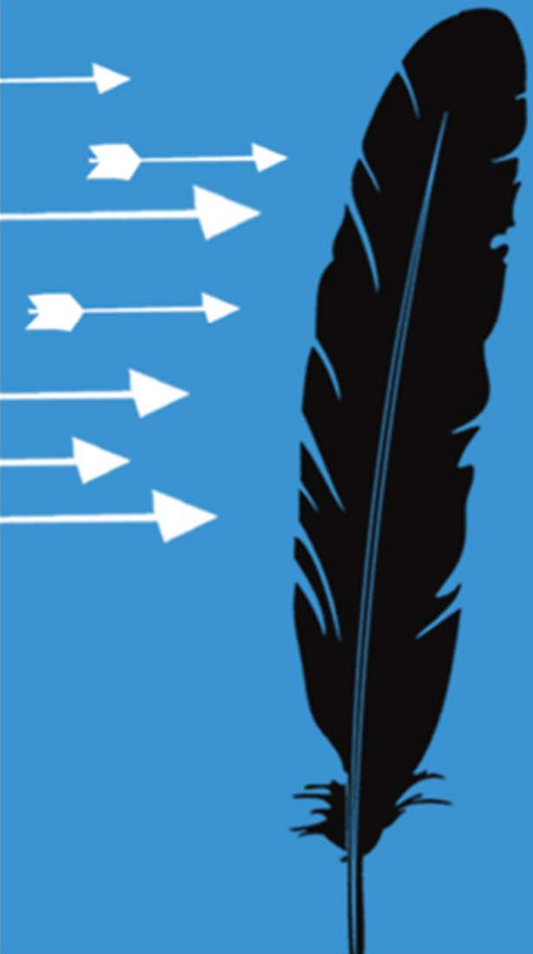
- Archiving & compliance
 - ActianceWorks, Arkovi, Socialware, Smarsh
- Content management
 - Syncapse, Vitruv, Shoutlet, Hearsay Social, Context Optional
- Monitoring & analytics
 - Radian6 (Salesforce), Sysomos, PostRank (Google), Alterian, Lithium Technologies, Collective Intellect, Crimson Hexagon



References

- New Media and the Air Force
- Parents' Guide to Facebook
- ENISA position papers
 - *Security Issues and Recommendations for Online Social Networks*
 - *Online as Soon as it Happens*
- ISACA
 - *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*
- *Securing the Clicks Network Security in the Age of Social Media*



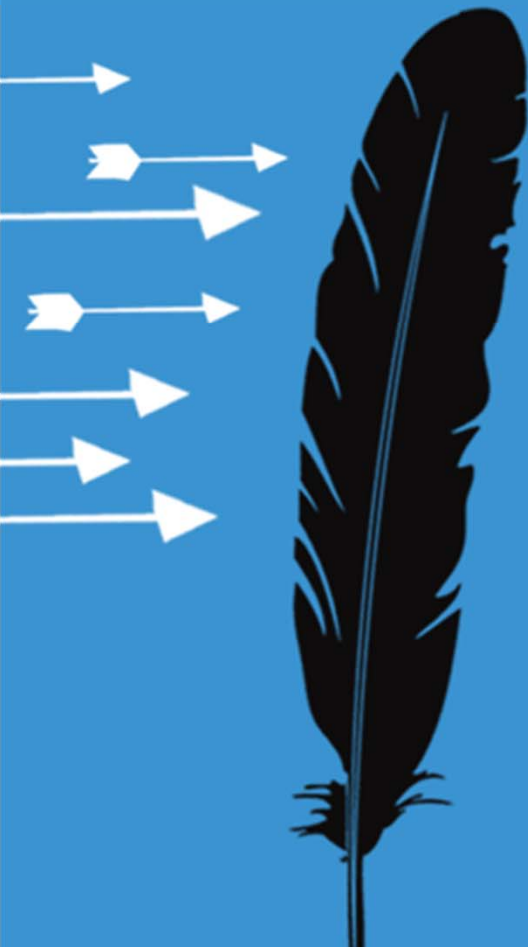


Apply

Apply

- understand how and why social media is used
- understand the risks you will face from not managing social media security properly
- implement security and privacy policies focused on the appropriate use of social media
- recognize social media security and privacy risks and take a formal approach to mitigate them





Ben Rothke, CISSP CISA
Manager - Information Security
Wyndham Worldwide
Corporation

www.linkedin.com/in/benrothke
www.twitter.com/benrothke
www.slideshare.net/benrothke