

Security Control for Utilizing Social Networking Sites

2012 FedCASIC Conference

March 29, 2012



NORC

at the UNIVERSITY *of* CHICAGO

Diana Salazar – NORC IT Security Compliance

- 20+ years in IT (consulted at 50 companies: Fortune 1000, small to large enterprises)
- 7 years as employee with NORC at the University of Chicago, federal contractor
- IT Engineering team managing: Enterprise Systems Security Program, System Architecture - Servers, SAN, VMware, Databases, Software Deployments
- Member – International Association of Privacy Professionals (IAPP), ISACA, TDWI – Board Member

- Infographics: Trends in Social Media Analysis
- Privacy and Legal Requirements
- Types of Searches
- Extracting Data
- Engaging Social Network Respondents
- Privacy Standards

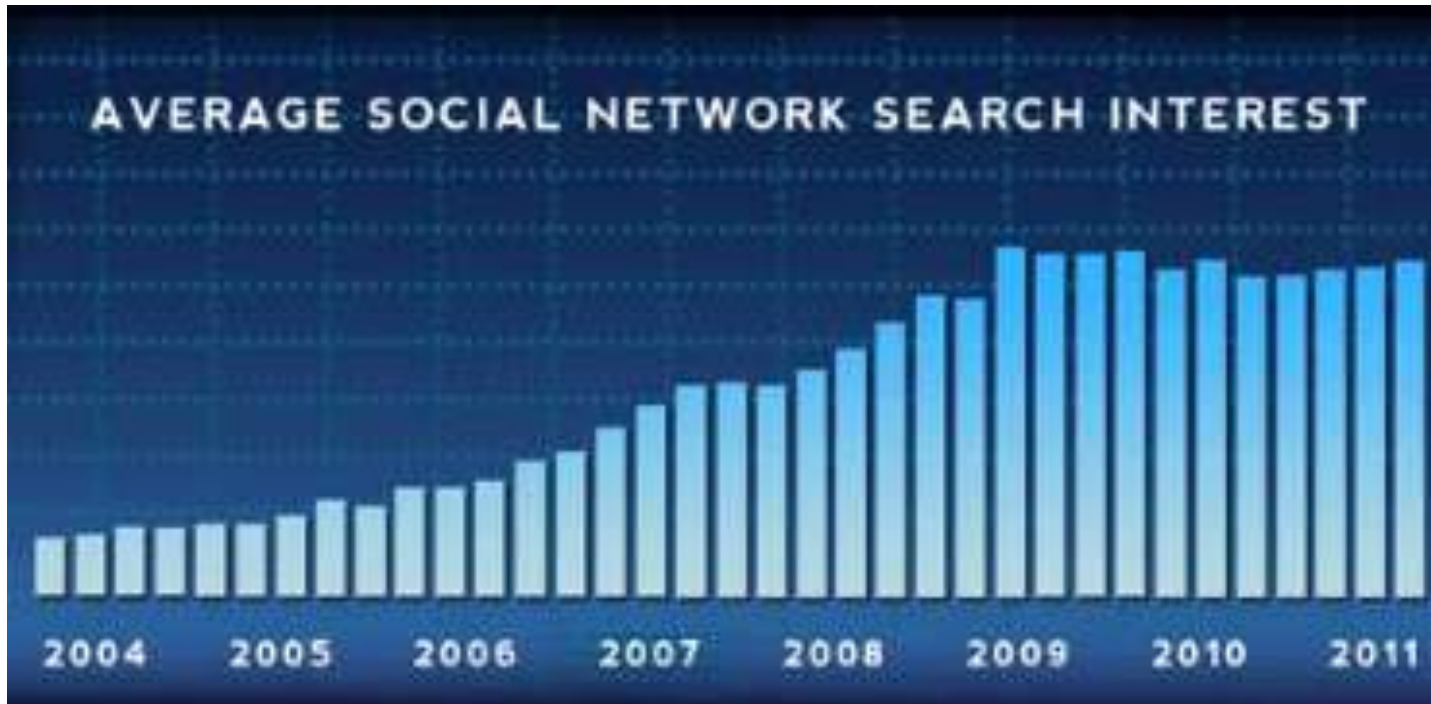
Why use Social Media Sites?

Locating respondents by traditional means has become increasing difficult due to:

- Dramatic increase in cell phone-only households
- Increasing mobility of younger respondents
- Increasing use of voice mail
- Calls are screened and more people are opting to be unlisted
- Less response to both traditional mail and email requests
- Individuals are more inclined to communicate through Social Media

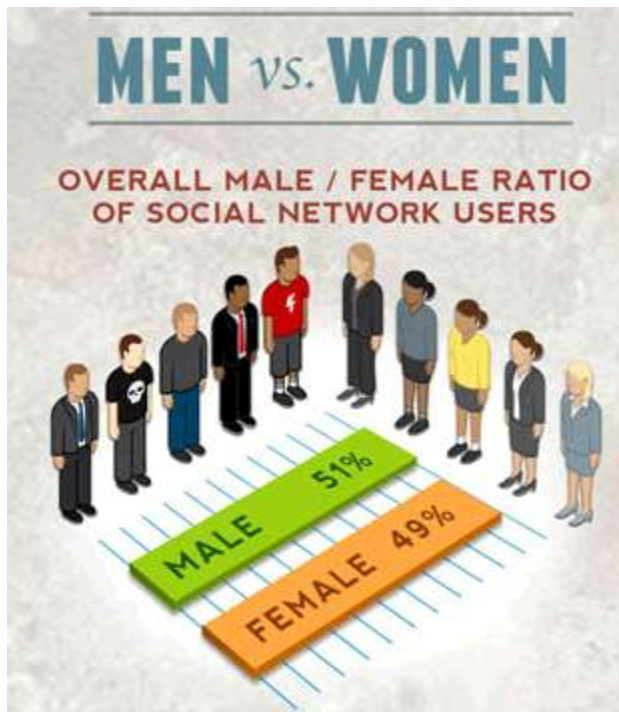


Social Networks Current State

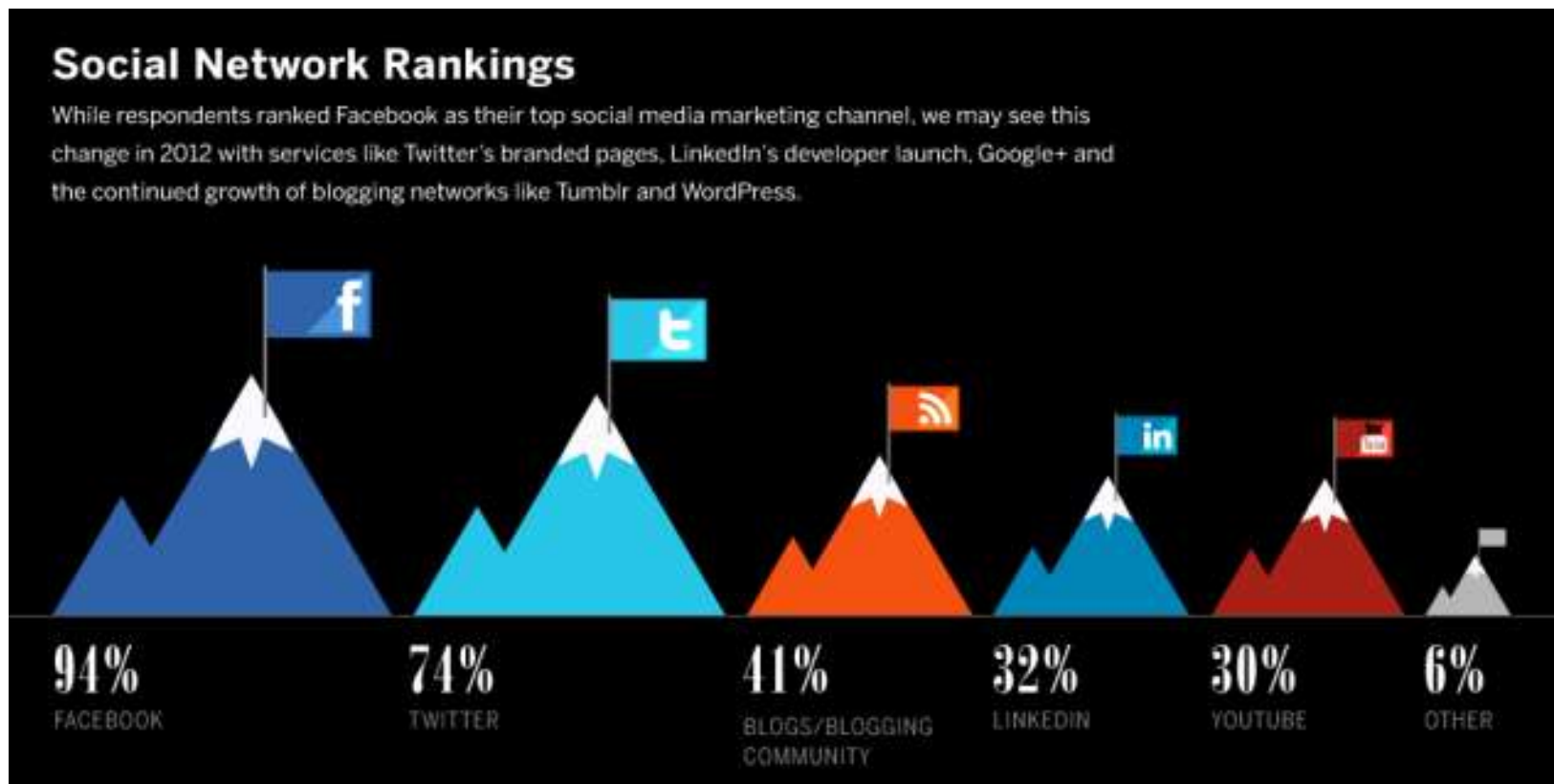


Infographic Trends

- Social networking sites can improve finding respondents



- Social Networks on the Rise



Types of Searches

Methods	
Manual	<ul style="list-style-type: none">• Name, school, city• Single threading• Does not allow use of use of all contact information• Does not allow easy search of individuals person-to-person links and affiliations• Searches of other publically available profile information are difficult
Active User Session	<ul style="list-style-type: none">• All API calls must be made within the session• Search results may not be stored or offered as aggregated search• User cannot be profiled• No data matching• Search results may not be stored or offered as aggregated search• Multiple people cannot search using the authentication credentials of one person. Each person must authenticate individually• Depending on the site and relationship there is limited number of searches per day per person.

Types of Searches

Search Methods

Automated

- Using an Application Programming Interface (API) provided by the site finds people using keywords, company, name, or other criteria. It returns a list of matching member profiles. Each entry can contain much of the information available on the person's member profile page
- The API can also return facets. Facets provide data about the collection of people, such as where they work, are located, or what schools they attended. This information can be used to make a new API call that further refines your original request.
- More information can be gathered through queries providing various parameter searches
- Information can be gathered about associate links

Extracting Data

Storage Methods

Database or File based

- Individuals consents through utilization of the site specific code allowing their data to be gathered
- Data elements need to be tracked with timestamp and site data was gathered from.
- Periodic wiping of disk needs to occur as part of maintenance process removing remnants of requested deleted data
- Access and audit controls for PII and sensitive data must be implemented

In-house systems

- Data can only be moved to in-house systems after consent
- Continued tracking and ability to remove data if requested by the individual

Social media is tough work... so finding opportunities to automate processes and reporting is essential to minimizing the impact of the resources needed. Over time, automating and integrating processes reduces the resource challenges allowing more time to focus on fine-tuning your strategy.

Engaging Social Network Respondents

- Legally binding agreements for sites by the developer
- Sites track all activity
- Respondents cannot be tracked to a particular study
- Cannot solicit respondents on the sites
- Security controls for consent, profiling, tracking data, and data matching
- Removal of data on demand

Engaging Social Network Respondents

- Agreements change continuously which require constant monitoring and adherence
- Create organization presence and ecosystem to provide link to your survey without identification
- Compensation can be done after proposed respondent leaves Social Media site
- Review requirements by each site regarding method of consent which may require their own consent code be deployed
- Limits on profiling, data matching and volume of queries
- Track data captured from what Social Media site for removal
- Have mechanisms to delete data and wipe underlying files on a frequent basis

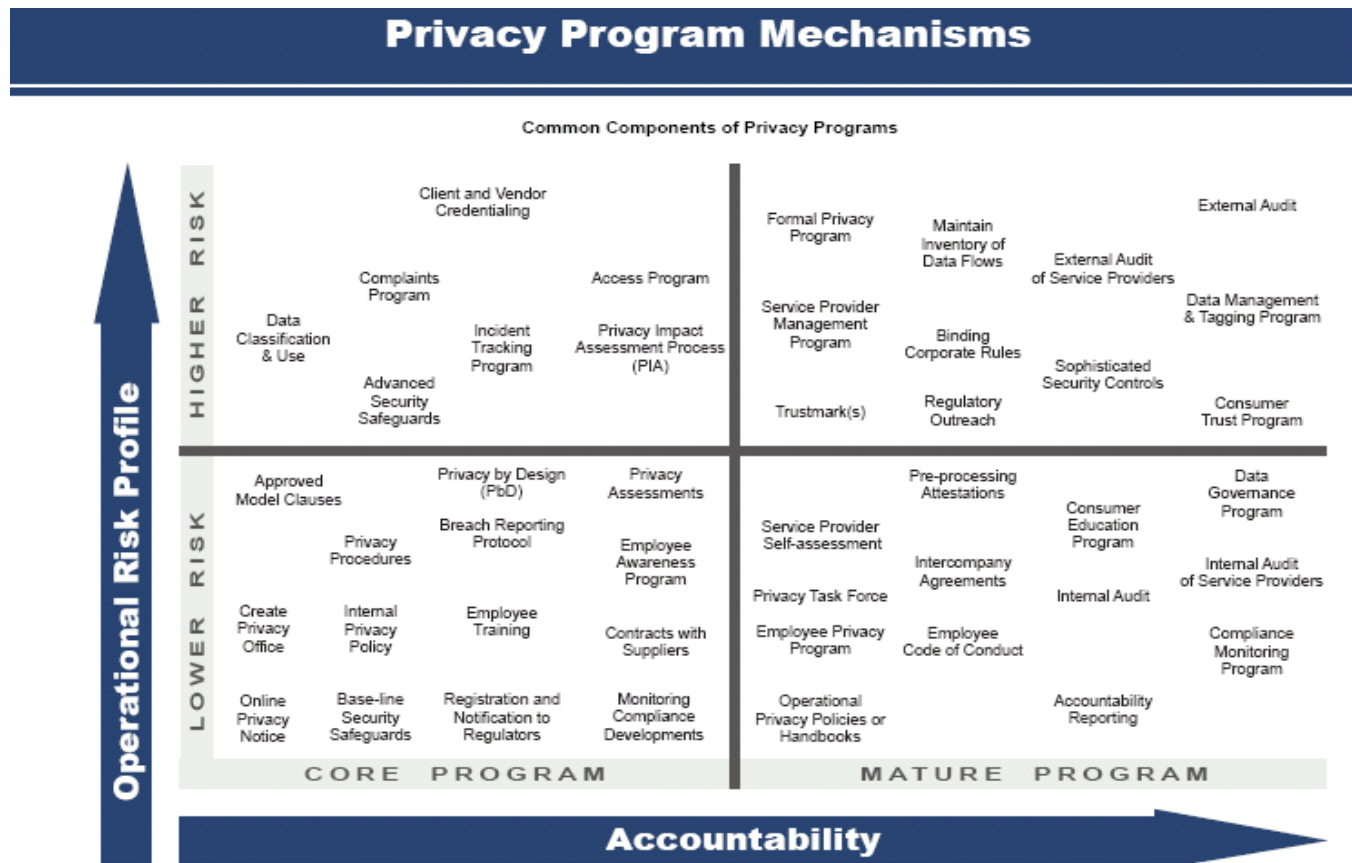
Engaging Social Network Respondents

- Use the Social Media Life Cycle

Social media provides valuable data for your business, along with a medium for conversation. These tools enable you to spot trends, opportunities and get insights, enabling you to act on some of those insights by participating in conversations that are going on and increasing your ROI.

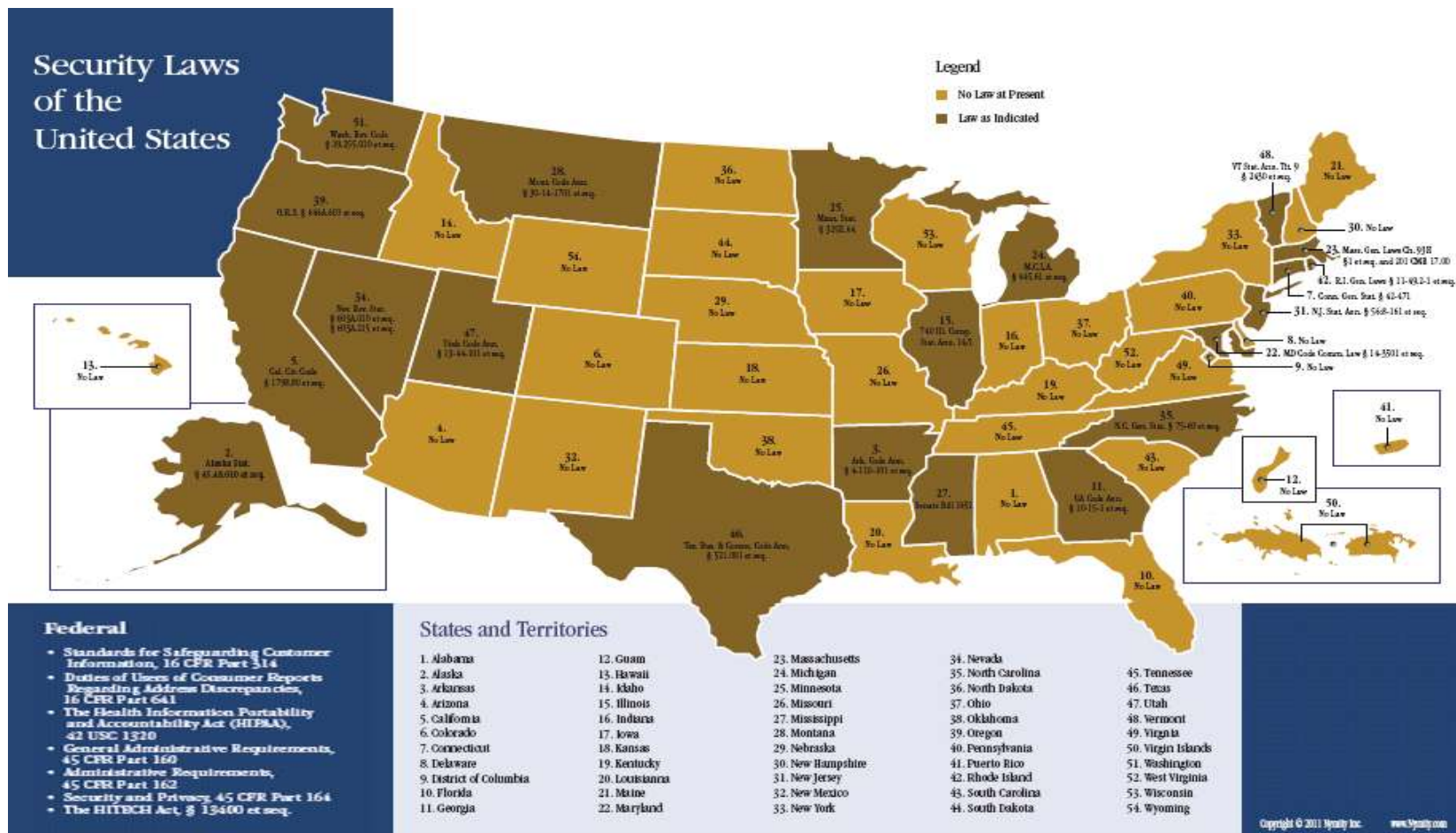


- Common Components in Privacy Programs



- Below is a list of regulatory schemes that may need to be part of a Privacy compliance framework:
 - [Consumer Data Privacy in a Networked World, Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012](#)
 - [Cybersecurity, Innovation and the Internet Economy, The Department of Commerce Internet Policy Task Force, June 2011](#)
 - NIST's Special Publication 800-53, Rev. 4, entitled [Security and Privacy Controls for Federal Information Systems and Organizations](#)
 - Guidelines on Security and Privacy in Public Cloud Computing, [Special Publication 800-144](#)
 - [CASRO Social Media Research Guidelines, Code of Ethics](#)
 - [Privacy Maturity Model \(PMM\), Assessment](#)

Privacy Standards



Diana Salazar – NORC Security Compliance
Salazar-diana@norc.org,312/759-2380

Thank You!



NORC
at the UNIVERSITY of CHICAGO

 insight for informed decisions™