

#PRIVACY

TWEET

LORI RUFF

FOREWORD BY WINN SCHWARTAU

Addressing Privacy Concerns in the
Day of Social Media

BOOK 01

A THINKaha BOOK

#PRIVACY **tweet**

Addressing Privacy Concerns in the Day of Social Media

By Lori Ruff
Foreword by Winn Schwartau

THiNKaha

E-mail: info@thinkaha.com
20660 Stevens Creek Blvd., Suite 210,
Cupertino, CA 95014

Copyright © 2010 by Lori Ruff

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means electronic, mechanical, photocopying, recording, or otherwise without written permission from the publisher.

Published by THINKaha™, a Happy About® imprint
20660 Stevens Creek Blvd., Suite 210, Cupertino, CA 95014
<http://thinkaha.com>

First Printing: November 2010
Paperback ISBN: 978-1-60773-088-0 (1-60773-088-X)
eBook ISBN: 978-1-60773-089-7 (1-60773-089-8)
Place of Publication: Silicon Valley, California, USA
Paperback Library of Congress Number: 2010939001

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Neither Happy About®, nor any of its imprints, can attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible. The information provided is on an “as is” basis. The author(s), publisher, and their agents assume no responsibility for errors or omissions. Nor do they assume liability or responsibility to any person or entity with respect to any loss or damages arising from the use of information contained herein.

Advance Praise

“What I love about this book is that it strikes a perfect balance between social media’s call to share personal information and sensible safety, for both the individual and the organization. Ruff shows you how you can be a social media rock star and still protect yourself from perverts, pirates, and other predators. A must-read for both IT decision-makers and anyone looking to build an online presence.”

Scott “Social Media” Allen, @ScottAllen, Coauthor *The Virtual Handshake, The Emergence of The Relationship Economy*, and <http://www.LinkedImage.com>

“Getting on board the social media train is no longer an option, but if privacy concerns are the reason behind your hesitation, Lori’s book is your ultimate guide to the do’s and don’ts of online privacy.”

John Antonios, @JohnAntonios, The Social Media & Personal Branding Blog

“Whatever you believe about online privacy and its implications on your life and business, this book will help you better understand what you need to believe.”

Jay Deragon, @JDeragon, Coauthor *The Virtual Handshake, The Emergence of The Relationship Economy*, and <http://www.relationship-economy.com>, one of the top 150 blogs in the world

“...a must read for any executive formulating a coherent social media policy for a corporation or concerned about their own online personal visibility. It’s full of practical advice and insight about the new world of social media driven conversations that are emerging as powerful forces that can harm or benefit.”

Lee Traupel, @LinkedMedia, CEO, Linked Media Group, Inc.

“We have heard the phrase “no man is an island” and “there’s no ‘I’ in team.” Think of social networking as a team of connected human beings following a set of rules that enables us all to be winners! Ruff helps you get comfortable and stay smart while making that happen.”

Bobby Didonato, @Mingle360, Director of Strategic Partnerships, Mingle 360

“Very relevant, entirely timely, proper perspective: all the elements you want when you’re going to learn.”

JoshuaABarnes, @joshuaatbarnes, Director of Information Technology, Socialmatica, Inc.

Dedication

This book is dedicated to
the person who wants to
enjoy all that the online
community has to offer but
who is vigilant to walk into
that world with care
and discretion.

Acknowledgments

Times have changed quickly and the pace of change continues to increase. Although the speed of our society accelerates, the essence of our humanity, civility, and decency cannot. I must therefore acknowledge the team that helped me to complete this project in record time in order to provide a highly requested resource for my fans and followers.

Thank you Mitch Levy (Happy About), *@HappyAbout*, for believing in this important project.

Thank you Janae Pierre, for your active and caring support.

Thank you Liz Tadman, for driving this project through to completion. You thought of everything!

Thank you Rajesh Setty, *@RajSetty*, for your brilliant editorial work.

Thank you Matthew Schnedl, *@RockTheWorldMgr*, you have proven yourself to be my favorite Booking Manager and a true Friend.

Thank you so much Winn Schwartau, for your support and advice and for believing that my voice will carry to the lay population about this important topic.

Thank you Mike O'Neil, *@MikeONeilDenver*, for supporting my effort and dedication and for sharing your passion for networking, for life and for me.

Thank you Steve Ruff; you are forever my biggest fan.

Why Did I Write This Book?

The reason I wrote this book mirrors the dedication found on page 5. As my partner and I travel the world speaking and training on LinkedIn and Social Media, people ask questions about privacy, about how to decide how much of or what kind of information it's OK to share, and how to protect themselves from attack.

This book is written from the perspective of someone who is passionate about online networking, yet I still had to make those same choices: how much of my life do I share? What areas am I comfortable talking about on a world stage? How to I protect myself from attack as my online presence grows? How do I help others as well?

I can't answer those questions for you. Each individual has to decide their comfort level. Two people with seemingly identical lives might make different choices. I have talked to experts in the security and privacy world and they all tell me the same thing: there are threats out there. Most people are ignorant of what the threats are and how to stop them. Not enough people care enough.

By raising the flag for awareness in the very public forum of social media, I have in essence staked my place as a spokesperson for the average social media user, to help them understand and offer at least a place to begin their journey.

Lori Ruff @LoriRuff, @LinkedInDiva

Contents

Foreword by Winn Schwartz	11
Section I	
Awareness	15
Section II	
Protecting Yourself and Others	39
Section III	
Healthcare Privacy	55
Section IV	
Timely Tips	67
Section V	
Privacy Tools	89

Addressing Privacy Concerns in the Day of Social Media

Section VI	
Resources	103
About the Author	111

Foreword by Winn Schwartau

Social Networking has linked three trillion people from seven satellite systems into a symbiotic reality that could not have been predicted even a few short years ago.

Business social networks. Personal networks. Friends and family. Industry specific. Talking to everybody even though they don't care you just brushed your teeth. And then there's the military and dozens of others...

What is the basis of any user's knowledge for proper behavior? We grew up with "Don't cross the street in the middle," "Don't drink and drive," "Don't take candy from strangers," but what about modern mantras that have not spread to the social networking masses?

- Don't say too much about yourself and your family.
- Do you really want to let the world know you're going to Bora Bora for a month?

Addressing Privacy Concerns in the Day of Social Media

- Consider carefully before job hunting in public forums.
- How do you avoid compromising pictures from parties that...well, you know.
- Kids being kids online can ruin their future opportunities.
- Are you being so dumb online that you have change your legal identity?

Knowing how to do something doesn't mean you should do it. Not knowing the repercussions of your online actions is even worse.

"Lori Ruff, The LinkedIn Diva," walks you through the good, tells you about the bad, and helps you avoid becoming the Ugly. Listen to the best advice you could hope for today.

Winn Schwartau

President, Interpact, Inc., Chairman, Mobile Active Defense, Author of *Information Warfare*, *Cyber Shock*, *Time Based Security* and *Internet & Computer Ethics for Kids*



Addressing Privacy Concerns in the Day of Social Media



Section I

Awareness

Knowledge and awareness can make all the difference. Timely advice alerts you to real privacy and online safety issues. Do you ever “Google” yourself? You might think you’re not online, you might think you know what’s out there, but go ahead and “Google” yourself—you may be “pleasantly” surprised.

1

Trying to reduce your digital footprint? Don't comment, share, like, connect, friend, or follow. Just lurk online. ;)

2

You can't hide in The Cloud. If you're going to participate in the online community, do it with deliberation & thought.

3

You need to maintain a balance.
Join the conversation; just do it
without a bullhorn.

4

When you “Like” a Facebook Page,
the page owner has the same access
to your profile as your friends.

5

Twitter? You can “protect”
your tweets to approved
followers only. But if you
mention anyone else,
they can see it too.

6

If a tree falls in the woods, you may not hear the sound, but if you post online, you can be pretty sure someone will see it.

7

Tweets mirror real life: use them for good. Report crimes, alert traffic monitors, mobilize voters, get the word out.

8

Are industry standards enough to keep you safe? Rarely. If you're concerned, read the fine print.

9

Government standards set the baseline. What's the best you can do to protect your clients?

10

Twitter bots spend time
Tweeting & RT'ing. Most
are not legit. Check out new
followers; report spam
when you see it.

11

An inappropriate question asked in a public forum requires an acknowledgement but not an answer in that same forum.

12

We're told that to be secure, we must give up privacy. Not completely: there are infinite shades of gray.

13

Being online is like being a player on a professional football team. You know you're being watched. Act like it.

14

It's easy to "over share" on social sites like Facebook. Before you "share," re-read your post.

15

Business professionals
need to be on LinkedIn and
engaged. Share only what you
would at your office.

16

Don't think Boomers aren't online.
They started the technological
revolution; they're business savvy
and online.

17

It took just one hour for Internet
experts to find out almost every
private detail of a woman's life. Via
Winn Schwartau

18

You need a panel to address social networking and privacy concerns. Make it diverse: Millennials, Gen-Yers, and Boomers.

19

Meeting new friends is easy online. Build a relationship and prove trust before you share sensitive information.

20

Keeping in touch with large numbers of friends is easy with Facebook and Twitter. Do you really want everyone to know?

21

Don't let emotions of good times or bad determine the level of your security precautions. "Later" is not the right time.

22

Privacy and security go hand in hand. You give up some privacy to be secure; you need to decide "how much" up front.

23

There will always be a time and place for you to shine. Don't miss the opportunity when it comes.

Via *@LauraLyseight*

24

The reality is that we are never guaranteed privacy. It is up to us to protect it, to secure it, to encourage it.

25

When is the last time you “Googled” yourself? Set up daily “Alerts” to raise your awareness.

26

How long before we have a candidate for President who grew up on Facebook? How will that change how we vote?

27

If celebrities are not immune from paparazzi, why should we expect to be immune from the “innocent sharing” of friends?

28

If you log into a secure site on a computer that is not your own, be sure you log out when you’re done.

29

Passwords are often guessed
by hackers watching what
you post online about your
life. Share with Care.

30

Concerned about security? Don't use your name as a social networking handle unless you are building a personal brand.

31

Common Sense Media provides common sense adage: "Self-reflect before you self-reveal."
Via *@JimSteyer*

32

“Digital citizenship” is everyone’s responsibility. Think before you type; think again before you post.

33

It is a criminal offense to invade the privacy of others. Intentionally humiliating people online often proves the case.

34

Just because you can upload and tag
a photo doesn't mean you should.
What you post online is a
permanent record.

35

Bullying is not only alive and well;
it is more common than you'd
hope. Call out cyberbullying: help
those attacked.

36

It's easier to become less private over time than vice versa, so err on the side of less, not more.

Via *@DaveTaylor*

37

The lines between public and private, personal, and professional are blurred in online social networks.

Via *@maltaee*

Addressing Privacy Concerns in the Day of Social Media



Section II

Protecting Yourself and Others

Dos and Don'ts to protect yourself
and others online, what to do, what to
avoid, who to believe.

38

Hackers will steal game passwords to steal your gold. You can be sure they will steal your business passwords as well.

39

Posting pictures online? Who's in them? Will they care that everyone can see?

40

If there's a problem with what people are saying online, address it where you found it, but resolve it privately.

41

You are the safeguard of your clients' data. Take extra care and report problems immediately.

Via @MikeOneilDenver

42

Climbers have maps and equipment. Prepare to navigate the digital terrain with software, policies, and common sense.

43

The premier online professional network is *@LinkedIn*. A “private” profile doesn’t guarantee people can’t see it.

44

Sites change policies
without telling you. Check
for updates monthly. At least
read the updates.

45

Plan security solutions and compliance policies that scale. If it works for 5, will it work for 10 or 200?

46

Compliance? Educate
employees on expectations,
perceptions, & best practices.

Most problems are caused
by ignorance.

47

When thinking Privacy, think levels of access, closed groups, and security measures.

48

Did your computer come with security software? Use it, keep it updated, run it on schedule. It will help save your A\$&.

49

Make sure you don't have anything visible online that is not professional.

Via *@immunechick*

50

Successful social media strategy = successful human relationships and conversations (in public!).

Via *@maltae*

51

Check your privacy settings
on every website and profile
with your name on it.

Via *@immunechick*

52

Your webmail client scans messages?
Your safety is not guaranteed.
Enhanced it with a local scan as well.

53

Firewalls protect you from cyber
attacks. Enhance yours with network
security tools and virus scanners.

54

Facebook privacy settings can be complex. Choose options carefully and preview effects of each choice before moving on.

55

We must be the voice of common sense in our circle of influence. Talk about privacy; invite others to join the dialog.

56

Protecting your tweets allows you to choose who sees your updates. People you tag can see what you say about them too.

57

Educate your family and friends about how you protect your privacy. Don't assume they know what to do.

58

If people lie, cheat and steal in the real world, they'll do it with vigor online. Practice caution and common sense.

59

When you trust your privacy to someone else, make sure they are transparent: Ask who gets to see what and why?

60

Do not disclose confidential or proprietary information on online platforms without appropriate approval. Via *@maltaee*

Addressing Privacy Concerns in the Day of Social Media



Section III

Healthcare Privacy

Doctors and nurses are not any more educated than you are about privacy in the social media space. Posting might seem innocent, but it often is not. Here's how to protect yourself and your patients.

61

Electronic Patient Health Records can improve quality of life and patient communication. Safeguard the tool.

62

HIPAA regulations? A place to start, but don't stop there. Educate healthcare workers in online etiquette.

63

The HIPAA Act of 1996 didn't see social media coming. It's still your job to keep information secure.

64

There is little professional guidance to help physicians navigate [social] connections with patients.

Via *@kboreilly*

65

Get a message and not the intended recipient? Unauthorized review, use, disclosure, or distribution is unethical.

66

Not only do pictures of patients NOT belong on Facebook, they don't even belong on your phone.

67

While healthcare professionals are taught effective medical skills, they need training to protect privacy online.

68

For privacy in medical offices, ask to discuss sensitive information away from reception. No cell phones please!

69

Should healthcare providers accept Facebook friend requests? It can advance patient health; just ensure that you keep postings professional.

70

Patients and doctors
or nurses connecting
on Facebook allow
progress monitoring and
communication between
office visits.

71

Providing health news related to your specialty on Facebook allows you to educate your patients en masse.

72

If patients ask specific questions on Facebook or Twitter, have them schedule a visit or correspond via encrypted email.

73

Posting ANY information that could identify a patient is unethical. Don't discuss patients in a public forum.

74

You don't engage your healthcare provider in a confidential conversation in public, don't do it online.

75

Not the intended recipient
of a confidential message?

Contact the sender
and destroy all copies
of the original.

76

Each individual has sole
responsibility for posts
published in any form of
online social media.

Via *@maltaee*

Addressing Privacy Concerns in the Day of Social Media



Section IV

Timely Tips

A look below the surface at some timely advice to help keep you and your business safe from attack and from irate customers!

77

Getting online from a public hotspot?
Other users can see your PC. Use with
caution and turn on the firewall.

78

If your reputation is important to you,
consider carefully before you post.
Think again before you hit “Publish.”

79

The strongest passwords are passphrases & numbers with no correlation to your life's events. Via Wynn Schwartau

80

Don't be lulled into trust. People ask for a little and a little more. Decide now where the line is so you recognize it.

81

Closing a browser session or shutting down a machine is not enough to stay secure: you must log out of your session too.

82

You can't hide from the issue. If your Head is in The Cloud, develop an EAR Policy for Education, Awareness, & Reporting.

83

Have a privacy team with diverse expertise to ensure your customer's POV. Don't forget a social media maven!

84

There is benefit for clients to access personal info online. That doesn't mean they want to share it with everyone.

85

Choose Company Privacy Settings. Through education and awareness, recommend settings for your employees. Say why!

86

Don't share company secrets to attract better clientele; but do give something of value to attract them.

87

Stated policy is essential to build trust with clients as well as to protect your business. Even better: provide proof.

88

Privacy questions do not have a one-size-fits-all solution. Although you can start with a standard policy, customize it.

89

Government regulations are minimum to ensure customer loyalty. Want real loyalty? Prove what you do beyond the basics.

90

If you're in a position where it is inappropriate to socialize with your clients, you shouldn't do it online either.

91

It is easy for a trusted business professional to collect information about their clients. It's harder to protect it.

92

Protecting confidential information includes checking and double-checking that you're sending info to the right party.

93

Your profile on sites like Mingle360.com allows you to identify how trusted a contact is and what info to share with each.

94

Providing industry news relevant to your clients lets you show your expertise and educate clients at the same time.

95

Use care when discussing client accounts in public forums. If you wouldn't talk outside the office, don't do it online.

96

Don't fear the negative feedback; instead, embrace it, learn from it, and deal with it. Via *@johnantonios*

97

Facebook is a community hangout. It's easy to forget where you are and say too much. If in doubt, keep it out.

98

Twitter is the world's publishing platform. Once it's in print, you can't take it back.

99

If your company site has a social element, engage as you would in person to maintain customer engagement.

100

Talking to prospects is what
drives business. Choose
appropriate online sites to
provide information easily
and securely.

101

Knowledge doesn't drive all success. Relevant content raises awareness of your expertise. Share appropriately.

102

Maintaining privacy on social networking sites requires you to be authentic. Decide what you want to share.

103

Those who don't understand
how technology works will
not likely understand the
implications of all their
actions online.

104

Privacy practices by
Customer Service can
work. Start with Education,
Awareness, Reporting. Ask
for customer preferences.

105

Have employees? It IS your responsibility to educate them on social networking protocols and how to avoid danger.

106

Denying access to sites at work is not enough to protect from privacy violations. Educate and raise awareness.

107

Social media has made you immortal,
but your legacy is your responsibility.

Via *@johnantonios*

108

LinkedIn is not a “social” networking
site. It is a professional gathering
place and should be treated as such.

109

Offline, bad becomes worse—Online,
bad becomes ugly—beware of the
viral effect of social media.

Via *@johnantonios*

110

When you mess up, be the first to
admit it and learn from the lesson.

Via *@maltaee*

Addressing Privacy Concerns in the Day of Social Media



Section V

Privacy Tools

The beginning of a collection of software, processes, education, and best practices.

111

Install, update & use firewall & virus scan to maintain maximum protection. Hackers don't take vacations.

112

Want Privacy for your group?
Consider a LinkedIn "Invitation Only" group and/or subgroup.

113

Ask how emails from your bank really look. If you get an odd one, call customer service before you click any links.

114

You owe it to your clients & partners to have your house in order; don't spread your cold!
Via @MikeOneilDenver

115

Do you know where your
USB sticks are? Always scan
removable drives that are
used on multiple computers.

116

When sharing or posting on Facebook, you have the option each time to select which group of friends can see. Choose it!

117

Become aware of tools to protect your privacy online while interacting in the social sphere. Implement what you can.

118

Learn how and where to respond to breaches of privacy online. Planning assumes you decide up front.

119

Technology delivers tiny devices that can transmit sounds and images. Have you scanned your environment recently?

120

In addition to firewalls and virus scanners, consider implementing tools that stop bots and block unwanted signals.

121

Use Google's "site:"
command to find/remove
rogue files and content
from your website.

Via *@MikeOneilDenver*

122

Simple passwords are not enough.
Create pass phrases mixed with
special characters and numbers to
enhance security.

123

Viruses, malware, and bots, Oh My!
Fight back with smart solutions from
trusted sources.

124

Because of rapid changes and upgrades, Facebook privacy settings should be checked monthly.

125

If you don't want people to tag you in photos on Facebook, change your settings to deny all or to require permission.

126

There is no better privacy tool than to be aware of what you share before you share it.

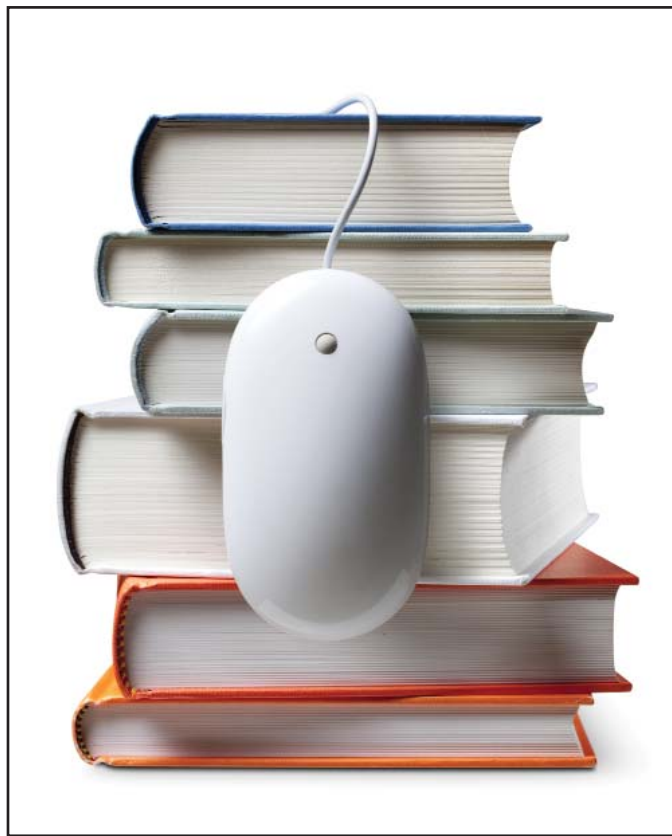
127

A plan is the foundation of your toolkit. You must have content strategy, social media strategy and policies in place.

128

Once you delete junk mail,
don't forget to empty the
trash. Malware will always
look for a way back in.

Addressing Privacy Concerns in the Day of Social Media



Section VI

Resources

Here are some great places to begin your search for help when you need it.

129

Where do you show up online? Track multiple sources (Bing, Google, Yahoo) to find them all.

130

Facebook Groups can send you messages and see your friends. How much did you intend to share?

131

Businesses: “It’s not enough
to be secure; you have to
prove you’re secure.”™—

NIST (Network Information
Security & Technology News)

132

Give employees a branded MingleStick to share contact info and marketing documents with the click of one secure device.

133

Internet safety group “Enough is Enough” offers education about online civility, cyberbullying, and internet privacy.

134

McAfee and other security packages often have site crawlers to help keep your website safe.

135

URL shorteners are great to save space. Use care when you click. Consider secure shorteners like <http://mcaf.ee>.

136

Electronic business cards like the Mingle360 allow you to “meet and greet” but control who gets what contact info.

137

The worst threat on social networking sites are malicious bots. Use network security tools like ThreatStop to stop them.

138

Use Google alerts and other tools to keep track of what people are saying about you online.

139

Use misspelled words to increase password security. For numbers, use a real or desired weight.
Via *@MikeOneilDenver*

140

Top Bands on the Radio:

*@LinkedIn, @Twitter,
@Facebook, @YouTube.*

Have you looked at their
#Privacy policies?

About the Author



The LinkedIn Diva, Lori Ruff, is a globally recognized expert in LinkedIn and social media. She is among the top 10 most connected woman in the world on LinkedIn. Her Facebook Friends list is full. Her robust Twitter following grows by hundreds of followers a week on three active accounts. You don't accumulate those kinds of social media credentials overnight. It takes years of active participation in the industry to earn a following like that.

Ruff is a proven thought leader with 100+ recommendations from clients and random people touched by her generous spirit. The Diva has heart, character, and avid fans with whom she has shared her knowledge. Over her career, she has presented over 1,000 sessions on topics such as leadership, social networking, fat applications and Internet technologies, customer service, and creating a vision, as well as privacy.

One sassy, saucy business woman, Lori is a full-time speaker, trainer, and co-author of the *Rock The World™* Book Series with her partner, The LinkedIn Rockstar Mike O'Neil.

Other Books in the THINKaha Series

The THINKaha book series is for thinking adults who lack the time or desire to read long books, but want to improve themselves with knowledge of the most up-to-date subjects. THINKaha is a leader in timely, cutting-edge books and mobile applications from relevant experts that provide valuable information in a fun, Twitter-brief format for a fast-paced world.

They are available online at <http://thinkaha.com> or at other online and physical bookstores.

1. *#BOOK TITLE tweet Book01: 140 Bite-Sized Ideas for Compelling Article, Book, and Event Titles* by Roger C. Parker
2. *#COACHING tweet Book01: 140 Bite-Sized Insights On Making A Difference Through Executive Coaching* by Sterling Lanier
3. *#CONTENT MARKETING tweet Book01: 140 Bite-sized Ideas to Create and Market Compelling Content* by Ambal Balakrishnan
4. *#DEATHtweet Book01: A Well Lived Life through 140 Perspectives on Death and its Teachings* by Timothy Tosta
5. *#DIVERSITYtweet Book01: Embracing the Growing Diversity in Our World* by Deepika Bajaj
6. *#DREAMtweet Book01: Inspirational Nuggets of Wisdom from a Rock and Roll Guru to Help You Live Your Dreams* by Joe Heuer
7. *#ENTRYLEVELtweet Book01: Taking Your Career from Classroom to Cubicle* by Heather R. Huhman
8. *#JOBSEARCHtweet Book01: 140 Job Search Nuggets for Managing Your Career and Landing Your Dream Job* by Barbara Safani
9. *#LEADERSHIPTweet Book01: 140 Bite-Sized Ideas to Help You Become the Leader You Were Born to Be* by Kevin Eikenberry

10. *#LEAN STARTUP tweet Book01: 140 Insights for Building a Lean Startup!* by Seymour Duncker
11. *#MILLENNIALtweet Book01: 140 Bite-sized Ideas for Managing the Millennials* by Alexandra Levit
12. *#MOJOtweet: 140 Bite-Sized Ideas on How to Get and Keep Your Mojo* by Marshall Goldsmith
13. *#PARTNER tweet Book01: 140 Bite-Sized Ideas for Succeeding in Your Partnerships* by Chaitra Vedullapalli
14. *#PROJECT MANAGEMENT tweet Book01: 140 Powerful Bite-Sized Insights on Managing Projects* by Guy Ralfe and Himanshu Jhamb
15. *#OPEN TEXTBOOK tweet Book01: Driving the Awareness and Adoption of Open Textbooks* by Sharyn Fitzpatrick
16. *#QUALITYtweet Book01: 140 Bite-Sized Ideas to Deliver Quality in Every Project* by Tanmay Vora
17. *#SOCIALMEDIA NONPROFIT tweet Book01: 140 Bite-Sized Ideas for Nonprofit Social Media Engagement* by Janet Fouts with Beth Kanter
18. *#SPORTS tweet Book01: What I Learned from Coaches About Sports and Life* by Ronnie Lott with Keith Potter
19. *#STANDARDS tweet Book01: 140 Bite-Sized Ideas for Winning the Industry Standards Game* by Karen Bartleson
20. *#TEAMWORK tweet Book01: Lessons for Leading Organizational Teams to Success 140 Powerful Bite-Sized Insights on Lessons for Leading Teams to Success* by Caroline G. Nicholl
21. *#THINK tweet Book01: Bite-Sized Lessons for a Fast Paced World* by Rajesh Setty

#PRIVACY TWEET

Privacy Explained So You Can
Network Online with Caution
but without Fear

"What I love about this book is that it strikes a perfect balance between social media's call to share personal information and sensible safety, for both the individual and the organization. Ruff shows you how you can be a social media rockstar and still protect yourself from perverts, pirates, and other predators. A must-read for both IT decision-makers and anyone looking to build an online presence."

Scott "Social Media" Allen, @ScottAllen, Coauthor "The Virtual Handshake", "The Emergence of The Relationship Economy", and www.LinkedinIntelligence.com, the most popular third-party LinkedIn blog

"Getting on board the social media train is no longer an option, but if privacy concerns are the reason behind your hesitation, Lori's book is your ultimate guide to the do's and don'ts of online privacy."

John Antonios, @JohnAntonios, The Social Media & Personal Branding Blog

"...a must read for any executive formulating a coherent social media policy for a corporation or concerned about their own online personal visibility. It's full of practical advice and insight about the new world of social media driven conversations that are emerging as powerful forces that can harm or benefit."

Lee Traupel, @LinkedMedia, CEO, Linked Media Group, Inc.

Lori Ruff, author, speaker and trainer, shows how you can secure your privacy at the individual, group and corporate levels with caution yet with confidence.



COMPUTERS & INTERNET, BUSINESS &
CULTURE, PRIVACY
\$19.95 US

THiNKaha

<http://thinkaha.com>

