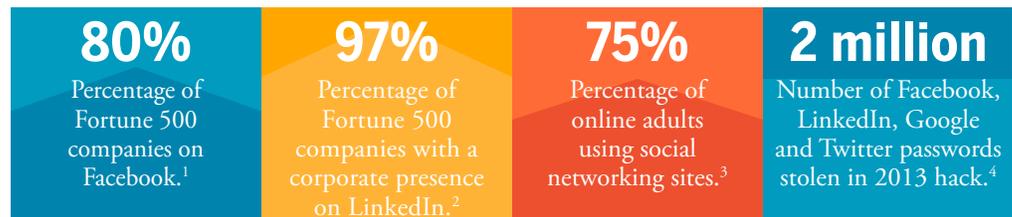


Global Data Privacy and Security Team

Social Media and Organizational Privacy Concerns: At A Glance

The majority of organizations utilize social media to market their products and services, interact with consumers, and manage their brand identity. Many mobile applications and websites even permit users to sign-in with their social media accounts and proceed to purchase items or use services.

While using third party social media websites has significant advantages for businesses, it also raises distinct privacy concerns. Specifically the terms of use that apply to social media platforms may give the platform the right to share, use, or collect information concerning your business or your customers. To the extent that the social media platform's privacy practices are not consistent with the practices of your own organization, they may contradict or violate the privacy notice that you provide to the public.



Bryan Cave's Global Data Privacy and Security Team has responded to hundreds of data security breaches and routinely helps clients, before a breach happens, analyze and improve upon their ability to respond to a breach if (or when) one occurs.

For more information contact:

Nicole D. Gates
Associate
nicole.gates@bryancave.com
120 Broadway, Suite 300
Santa Monica, CA 90401
phone: 310 576 2205

Andrew W. Klunness
Partner
andrew.k@bryancave.com
120 Broadway, Suite 300
Santa Monica, CA 90401
phone: 310 576 2176

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6000

For additional information,
please visit
www.bryancavedatamatters.com

What to consider when evaluating your organization's use of social media:

✓	How would a data breach of social media platforms affect your organization? Do you have a plan if your social media account is breached?	✓	Do users log in to your services or make purchases through a social media platform?
✓	Does your organization share information with an intermediate service provider, such as a social media analytics company, to provide or analyze social media services?	✓	What type of PII do your customers share with you on social media platforms?
✓	Is your internal data or customer PII protected by the terms of agreements with third parties, including social media platforms' terms of service?	✓	Does your website's privacy policy and terms of service make clear that social media platforms are third party websites?
✓	What types of customer PII are solicited, collected, maintained or disseminated via your social media platforms (e.g., geo-location)?	✓	Does your use comply with the platform's policy for collecting data from users? Do you review these platform policies regularly?
✓	Do you display information or images of users or other people (including your employees)? Did the people give permission and/or sign a release?	✓	Does your organization have a social media policy governing employees' use of social media, particularly pertaining to sharing confidential customer and organizational data?
✓	Is your client list private? Do your employees connect to your clients on social media?	✓	Do you work with your IT team to manage security and passwords of your social media sites?
✓	How is information about your customers collected from social media sites being stored? Do any third parties have access and for how long?		

¹ <http://www.umassd.edu/cmr/socialmediaresearch/2014fortune500andsocialmedia/> (last viewed April 2015).

² <http://www.umassd.edu/cmr/socialmediaresearch/2014fortune500andsocialmedia/> (last viewed April 2015).

³ <http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/> (last viewed April 2015).

⁴ <http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/>; <http://www.cnet.com/news/researchers-discover-database-with-2m-stolen-login-credentials/> (last viewed April 2015).