Legal and Ethical Issues in Social Media 11

This chapter takes the perspective of legal and ethical issues in social media to complete the multidisciplinary approach of this book. Instead of intending to give legal advice, this chapter encourages the reader to reflect on proper social media use. Previous chapters already looked at how legislation is related to social media. Particularly, the chapter on online ads (Chap. 4) talked about privacy and cookie laws. Furthermore, the chapter on e-recruitment (Chap. 9) discussed some legal practices for getting not recruited or for getting fired because of social media posts. The chapter on crowdfunding (Chap. 10) referred to legislation to protect micro-investors. Besides legislation, also ethical concerns have been formulated. For instance, the chapter on SEO mentioned the use of black hat SEO techniques (Chap. 6), and the chapters on business intelligence considered the impact of fake customer reviews (Chap. 7) and privacy concerns for big data analysis (Chap. 8). This chapter supplements the previous chapters by discussing social media ethics from the perspective of organizations, as well as the perspective of individual employees as social media users. The reader learns about the role of a social media policy, Terms of Service, copyright or intellectual property, a digital after-life, and password security, among others.

This chapter turns to the legal department within an organization in order to complete the multidisciplinary approach of social media (Fig. 11.1).

11.1 Introduction to Legal and Ethical Issues in Social Media

Suppose you are a blogger who frequently blogs about new technologies. Being a key influencer in the IT community, you are contacted by a software company that asks you to write a supporting blog post about its new product. What would you do?

In order to act in an ethical way, a supporting blog post can still be published if you mention that the company requested for this (or even paid for it). Or, as an independent blogger, you can write personal opinions about the offered product,

A. Van Looy, *Social Media Management*, Springer Texts in Business and Economics, DOI 10.1007/978-3-319-21990-5_11

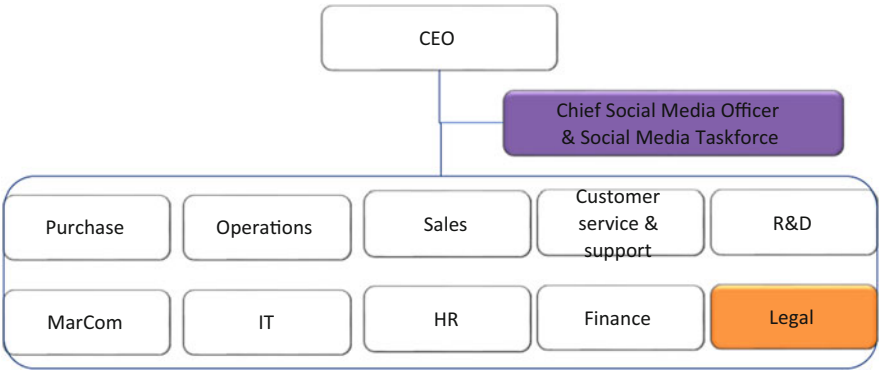

Fig. 11.1 The multidisciplinary approach of legal and ethical issues in social media

which possibly contain negative aspects too. Similar to online ads, a writer's affiliation should be disclosed in every type of supportive message that could influence the purchasing decisions of customers (Word of Mouth Marketing Association 2014). Hence, in this example, disclosure of relationship is relevant to the blog readers who might get influenced to purchase the product.

Social media ethics imply that a social media user should be honest about his/her relationship, opinion, and identity. For instance, some examples of nonethical behavior from the perspective of organizations are:

- Blog posts or brand reviews paid by marketers, who are hired by an organization
- Ghost tweeters
- Fake customer reviews
- Fake chat room members
- Viral campaigns that pretend to be user videos
- Etc.

But also employees can act in an unethical way, for instance, by:

- Revealing business information online
- Insulting clients or colleagues online
- Posting obscene photos about their spare time
- Etc.

Such examples may seem obvious at first sight, but many people post information online without giving it a lot of thought. In both professional and private situations, unethical social media use can harm the employer (see e-recruitment, Sect. 9.4). Therefore, individuals should always be careful when posting pictures about their hobby as a stripper, being drunk at a party, "liking" posts that deal with alcohol or drug abuse, etc.

Social media ethics have become a highly important topic, because social media are rapidly increasing in use and tend to blur the boundary between someone's

private life and professional life. An unclear line also exists between freedom of speech and inappropriate posts. Due to the potential dangers related to social media, the need for education about proper social media use is increasing. Examples of potential dangers of social media use for organizations and employees are as follows (Association of Corporate Counsel 2010; HR Examiner 2013; Reynolds 2010):

- **Privacy**: see Chaps. 4, 8, and 9 (Bélanger and Crossler 2011).
- **Discrimination**: see Chap. 9. Social media posts can give digital evidence of discrimination or harassment.
- **Copyright:** an employee should not just copy and post someone else's work (e.g., text, video, picture, poem, art, etc.) without requesting the owner's permission (see also Sect. 11.3.2 on digital afterlife).
- **Intellectual property**: this danger refers to the question whether social media content is owned by the employee, the employer, or the social media tool (see also "Terms of Service," Sect. 11.2.2). Furthermore, an employee should not post business secrets online. Another example concerns the ownership of online contacts that a recruiter or salesman has while performing his/her job. Particularly, an agreement can be made that stipulates who will get a copy of the social media contacts when this employee leaves the organization.
- **Terms of Service:** if an organization opens an account on one or another social media tool, it needs to accept the tool's Terms of Service (see Sect. 11.2.2). In order to fully understand what the organization actually signs and which legal consequences are related, a legal advisor can be consulted first.
- **Disclosure of relationship:** when posting information online, an employee should disclose whether or not he/she acts as an employee of the organization and thus gets paid to create online ads, viral campaigns, blog posts, reviews, etc. (see supra).
- **Disclosure of location:** an employee or employer can also indirectly reveal business secrets by mentioning his/her location online (see also "intellectual property"). For instance, by using a tool such as Swarm™, social media connections may know when the employee is at work and not at home (e.g., if burglars are followers) or how many times an employer checks in at a certain airport or in a certain city (e.g., journalists can derive when strategic discussion are going on with competitors or suppliers who are located on a specific location).
- **Defamation**: if an employee publishes false information or lies about someone to damage the reputation of that person, the organization can be liable for it in some situations (e.g., if the information is published on the corporate website).
- **Office drama**: as social media posts can be easily sent (and also outside working hours), an employee may post something without common sense and so hurt or embarrass colleagues (e.g., when the employee is angry, sad, tired, drunk, etc.).
- **Etc**.

It is important that both employers and employees are aware of these potential dangers that directly or indirectly relate to social media use and that may impact on an organization's reputation. Although ethical behavior strongly depends on a relationship of trust, organizations can also educate their employees to recognize such dangers and teach them how to act professionally in diverse situations. A possible way to discipline employees is by means of a social media policy, supplemented by training (Flynn 2012).

Consequently, a secret to success in social media (and business ethics in general) is building trust. As discussed in Chap. 5 on social CRM, it concerns trust between the employer and its employees but also with its suppliers and customers and above all with its fans on social media (i.e., who are different from customers, but may be prospects or influencers). By building trust, the organization will be more likely to save its brand, reputation, and jobs when, for instance, a crisis hits. Particularly, good relationships with stakeholders can serve as a buffer in times of crisis. This means that an ethical use of social media can facilitate online reputation management and even crisis management afterwards. Furthermore, SEO (see Chap. 6) can help reputation management in order to facilitate sharing (ethically correct) corporate information (e.g., press releases) and to make the corporate website more adapted to the requirements of search engines, social media, and smartphones.

11.2 Social Media Ethics by Organizations

This section elaborates on the explicit actions that an organization can take in order to encourage ethical behavior on social media. Particularly, in addition to building trust, an organization can create a social media policy (or a social media code of ethics) with a corresponding training program (Institute of Business Ethics 2011; SocialMedia.org 2010). Furthermore, it should take into account the Terms of Service of social media tools. These actions are subsequently discussed.

11.2.1 Social Media Policy and Training

A social media policy is often part of a larger IT policy on business conduct. An organization can create a social media policy from scratch, or it can rely on ethical communication guidelines of industry associations (Postman 2009). Templates, guidelines, and examples of social media policies can also be found in a social media policy database (e.g., Boudreaux 2014). One example is the social media policy present at Ford™: http://www.scribd.com/doc/36127480/Ford-Social-Media-Guidelines. Another example concerns IBM™'s social computing guidelines, which were created by means of crowdsourcing (see Chap. 10) among the employees: http://www.ibm.com/blogs/zz/en/guidelines.html. Besides addressing the potential dangers mentioned in the introduction section, a social

media policy may consider the following elements (Institute of Business Ethics 2011; SocialMedia.org 2010):

- **Social media (policy) audit**. Chapter 3 explained that social media use should follow a social media strategy, which serves the organizational strategy. Hence, social media should only be used if they can help reach the business objectives or solve business problems. In order to know which problems are to be solved and by which principles, a social media audit can be performed with a survey and/or in-depth interviews of employees (Borremans 2013). An audit may, for instance, also uncover whether employees use social media in an ethical way, whether they are aware of the social media policy in the organization, or whether the managers have an accurate idea of the online behavior of employees. Such insights may be used to set a social media policy or to recommend additional training. An example of a social media policy audit survey is given in Flynn 2012.
- **Communication principles and standards**. A social media policy contains principles about the way employees are ought to act, which should be consistent with the corporate values. For instance, a social media policy can be explicitly driven by corporate values, e.g., collaboration, transparency, diversity, respect, and quality (e.g., http://www.coca-colacompany.com/stories/online-social-media-principles#TCCC). Furthermore, a social media policy can set the organization's online voice and tone. For instance, it can define the expected response time (e.g., an organization can commit itself to respond to answers on Facebook™ within 16 h, on Twitter™ within 2 h, and to emails within 24 h). Also possible characteristics of the organization's voice can be defined. For instance, if the voice is set to approachability, curiosity, and knowledge, then social media posts will rather be conversational, using exciting words and providing casual information.
- **Chief Social Media Officer.** As discussed in Sect. 1.3, a dedicated job description for a Chief Social Media Officer is rising in organizations. Having the right people in charge of social media is crucial. It does not necessarily concern people under the age of 25 who use social media a lot (i.e., generation Y), as older people may have relevant experience with marketing principles and knowledge about the business (Borremans 2013; Forbes 2012). Hence, an organization should hire someone who has both business savvy and social media savvy (e.g., great writers and storytellers), but regardless of their age.
- **Social media monitoring and training.** In line with Chap. 3 on social media strategy and ROI and with Chap. 5 on social CRM, an organization should regularly review its social media dashboard metrics. Monitoring social media conversations also enables an organization to correct people's misstatements related to the organization (SocialMedia.org 2010). For instance, see Chap. 7 on opinion mining. Monitoring can generally be considered as an ethically correct action, as long as it is announced in a (social media) policy and that the people involved are aware that monitoring takes place (Institute of Business Ethics 2011). Similarly, if an organization blocks certain websites or social media tools,

it should be clearly stated in a policy. However, trusting employees might be an alternative to actually blocking sites, e.g., by hiring people that fit the organization and by regularly training them (Stop Blocking! 2010).

- **Disclaimers.** It should be clear whether an employee is either representing himself/herself or his/her organization when using social media to talk about the organization and its products or services. The former would imply that the social media content represents his/her personal opinion or contribution. In case of the latter, an employee is participating in social media on behalf of the organization and should rather get the manager's approval first. For transparency reasons, an employee should particularly provide a disclaimer if using a tool that is not sponsored by the organization, even if disclaimers are not explicitly requested by an organization in the organization's social media policy. For an example of a social media policy that explicitly requires disclaimers, have a look at the policy at Dell™: http://www.dell.com/learn/us/en/uscorp1/corp-comm/social-media-policy?c=us&l=en&s=corp&cs=uscorp1. Hence, a disclaimer is a disclosure of relationship and can be seen as a declaration whether the social media user represents or has an interest in a specific organization (Word of Mouth Marketing Association 2014; SocialMedia.org 2010). In the end, it should be clear whether social media are used by the organization or privately by an employee for personal use. Aspects that can be mentioned in a disclaimer are the person's name, whether he/she was paid for posting the related content and thus represents the organization's point of view, or whether it concerns his/her opinion based on a real experience. Some examples of disclaimers are given for the reader's information in Table 11.1.

11.2.2 Terms of Service of Social Media Tools

While organizations can set their own social media policy, each social media tool can set its own Terms of Service. As mentioned in the introduction of this chapter, organizations or individuals can only make use of a social media tool after accepting the tool's Terms of Service. These Terms of Service define what the social media tool can offer (i.e., as a service) and how it should be used. The latter explains why the notion "Terms of Service" can also be called the "Terms of Use" and generally stipulates the policy agreements regarding privacy, copyright, cookie use, safety, etc. As an illustration, we hereby give the link to some examples of Terms of Service:

- https://www.facebook.com/legal/terms
- https://about.pinterest.com/en-gb/terms-service
- https://twitter.com/tos
- https://support.twitter.com/articles/41949-guidelines-for-law-enforcement

While the Terms of Service can be considered as general information for the users, additional guidelines for law enforcement authorities can be given on a

Table 11.1 Examples of disclaimers

Example for social media posts in general: "Hello! My name is Valentina and I work for organization XYZ." "These posts are my own, not those of organization XYZ."
Example for a blog sponsored by organization XYZ: "Some of the authors contributing to this site, [including the moderators,] work for organization XYZ. Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, not those of organization XYZ."
Example for a third-party blog: "The opinions expressed in this blog are my own views and not those of organization XYZ." or "I received product X or information Y from Organization ABC. #paid"
Example for the personal blog of an employee (Borremans 2013): "This blog is a personal blog written and edited by myself. For questions about this blog, please contact me. This blog does not accept any form of cash advertising, sponsorship or paid topic insertions. However, I accept and keep free products, services, and travel or event tickets from organizations. However, those free products, services, travel or event tickets will never influence the content, topics or posts made in this blog. The views and opinions expressed on this blog are purely those of the blog owner. I will only endorse products or services that I believe, based on my expertise, are worthy of such endorsement. Any product claim, statistic, quote or other representation about a product or service should be verified with the manufacturer or provider. This blog does not contain any content which might present a conflict of interest."

separate web page (e.g., https://support.twitter.com/articles/41949-guidelines-for-law-enforcement).

According to the user rights initiative "Terms of Service; Didn't Read" (2013), most people do not read the Terms of Service when signing up for an online mailbox or a social media tool or when downloading an app and just give their approval. Although the Terms of Service may impact on someone's online privacy, people tend to agree because the Terms are often perceived as too long and written in legal terms. Therefore, the initiative "Terms of Service; Didn't Read" (2013) developed a rating and labeling systems for Terms of Service and privacy policies on the Internet. The ratings vary from very good (class A) to very bad (class E). Many social media tools have already been rated so far, and the results are publicly available. Hence, this initiative allows people to become more aware of what they sign up for.

An important issue related to the Terms of Service of social media tools concerns **intellectual property**. This broader issue relates to the ownership of social media data, i.e., whether the published content is actually owned by the social media tool, the employee, or the employer. Most social media tools give nonexclusive rights to its users, which means that a user may retain all rights and is solely responsible for his/her UGC. Nonetheless, many social media tools also stipulate that they can reuse a user's content and pictures for commercial and audit purposes, even when the content or picture is removed by the user. Also other users who have shared specific content or a picture might still be able to make use of it after deletion by the

user. This implication illustrates that social media posts can be considered as undeletable (see Sect. 1.2).

Another topic related to intellectual property is **copyright infringement** and implies that a social media user should never copy any content that is created by other people or organizations without acknowledging the original source. Still, the ease of posting on social media tools entails the risk for a user to pretend that a certain post is his/her own creation (e.g., a slogan, a video, or an article), even if it does not concern the user's original work. Particularly, pictures on Google™ Images, YouTube™ videos, or lyrics are not there for the taking, and at least the original source should be mentioned. When the original source believes his/her copyright-protected work was posted on social media without authorization, a copyright infringement notification can be submitted to the social media tool (e.g., http://www.youtube.com/yt/copyright/). We must, however, note that a copyright infringement differs from just "sharing" or "liking" information, which generally does not need prior approval.

11.3 Social Media Ethics by Employees

From the perspective of employees, it is interesting to regularly check which online information is publicly available about yourself as an individual. For instance, in Chap. 9 on e-recruitment, the reader was invited to look for his/her own name in a search engine and to take actions if necessary. Such personal searches are not merely conducted by recruiters. Also other jurors can and will screen someone's online identity (e.g., colleagues, customers, suppliers, competitors, etc.). By doing regular "me" searches, employees can manage which personal information can be found by other people. Hence, online reputation management is also important to employees.

Different theoretical approaches exist to assess whether something is ethically correct or not. Ethical frameworks generally distinguish the following approaches (Jain 2013; Velasquez et al. 2009):

- **Utilitarian approach**: ethical decisions will choose for behavior that maximizes utility, i.e., which is most useful or most positive with regard to its outcomes or consequences for all stakeholders ("the greatest good to the greatest number").
- **Rights approach**: ethical decisions will choose for behavior that best protects and respects the rights of all stakeholders.
- **Fairness and justice approach**: ethical decisions will choose for behavior that treats stakeholders equally or proportionally.
- **Common good approach**: ethical decisions will choose for behavior that best serves the community as a whole, instead of only the stakeholders.
- **Virtue approach**: ethical decisions will choose for behavior that best reflects some virtues or ideals in order to reach an individual's highest potential (e.g., honesty, courage, compassion, integrity, generosity, tolerance, etc.).

- **Principle approach**: ethical decisions will choose for behavior that best fits a specific code of ethics, i.e., by applying personal, professional, or global ethics.

Subsequently, this chapter provides the reader with practical considerations regarding an individual's online behavior.

11.3.1 Do's and Don'ts for Social Media Use

Online behavior of individuals may refer to business use or personal use. In both situations, employees should respect some general do's and don'ts (Jain 2013; Institute of Business Ethics 2011).

Examples of ethical do's and don'ts for employees are:

- **Policy**. When communicating anything related to the organization, employees should act in accordance to the organization's code of ethics (i.e., the social media policy and more generally the policies on IT and business conduct).
- **Permission**. When communicating anything related to the organization, employees should first ask their manager for (oral or written) permission. Written permission is particularly required when it concerns confidential or copyrighted material (i.e., that belongs to current or former employers or third parties). Furthermore, identifiable client information should not be posted online without client's permission.
- **Confidentiality and professionalism**. Additional to the policies, some organizations can ask their employees or interns to sign a nondisclosure agreement. Nonetheless, confidentiality should always be contained regarding "internal use" information, and business secrets should not be publicly revealed. Similarly, employees should avoid public statements about the financial performance of current or former organizations.
- **Reputation management.** Employees should contribute to online reputation management to protect both the organization's and their own reputation. Also private social media use should be considered from this perspective (e.g., when clients or colleagues are personal connections or when personal social media posts are in the public domain).
- **Privacy**. Individuals should set privacy setting to safeguard private content. Employees should act professionally, also in their spare time. In order to maintain appropriate professional boundaries, different accounts can be created to separate their private use of social media from their professional use (i.e., a personal online identity versus a professional online identity).
- **Discrimination or harassment**. During and outside working hours, employees should avoid vulgar, discriminating, or unflattering content on any website or account. Discrimination has a broad interpretation, among others disrespect for someone based on age, race, gender, ethnicity, sexual orientation, etc. Furthermore, caution is required for content that relates to (an abuse of) alcohol and drugs.

- **Informal social control**. Employees should bring unethical content or behavior to the attention of a manager or the colleague involved.

11.3.2 Digital Afterlife

A topic indirectly linked to social media is the digital afterlife of individuals, i.e., what happens with someone's social media content and accounts when that person dies? To have their digital data properly managed, social media users (or Internet users in general) can take some precautions in a so-called digital will. Although this topic may seem awkward at first, some things in life should be given a thought from time to time.

A first question to be considered is whether your legal heirs (i.e., your loved ones) are aware of all your social media profiles and content. If so, can they also access them? Or maybe the content is not readable anymore, because the file format has changed over time (e.g., from PDF files to a new document extension in the future)? Another question concerns the ownership of social media data (Carroll and Romano 2010; The Digital Beyond 2010). The latter question deals with copyright issues and the discussion on Terms of Service (see Sect. 11.2.2). Copyright can last for the life of an individual creator plus 50–70 years (Wikipedia 2014). This implies that social media content (e.g., pictures or recordings) can be registered together with other valuable assets (such as a house, furniture, or personal properties).

Social media tools do not necessarily give legal heirs access to the profile of a deceased person. Hence, a relatively safe solution is to provide a list of network usernames and passwords to a trusted relative or friend. Some commercial organizations try to make money in this area and let you (regularly) pay for their service (Social Media Explorer 2014; Vuze 2013). Meanwhile, social media tools start having a policy about account settings. For instance, in 2011, Google™ launched its "Inactive Account Manager" feature to proactively create a digital will related to the person's Google™ services in use (CNET 2011). This feature allows, for instance, to set a time-out period (e.g., after 3–12 months of inactivity) and to send automatic notifications to the users and/or his trusted contacts when the time-out period ends, including the possibility to automatically delete the user's account after a predefined period of time (https://support.google.com/accounts/answer/3036546). It is to be expected that social media tools will increasingly offer a solution to a user's digital afterlife in the future.

11.3.3 Privacy and Passwords

Following the section on digital afterlife, an option exists to look at your online presence and to list up all your online memberships with corresponding username and password. If this option is chosen, the list should be regularly updated as login

details can change over the years. The list should also be safely stored and only for your trusted ones to be found. Such a paper-based list might be the easiest way to manage a digital afterlife without additional costs, but should not be saved on a computer (i.e., due to the related security risks).

Given the relevance of passwords for proper social media use, this section gives some general tips and tricks to create strong passwords (BullGuard 2013; Burnett and Kleiman 2006; Intel 2013).

- **Creation**. Internet users should choose passwords of at least eight characters long, which are rather non-words instead of names (e.g., not your pet's name), instead of dictionary words (e.g., not "password" or not "admin"), or instead of words spelled backward (e.g., not "drowssap" which refers to "password"). Also avoid common character sequences (e.g., not "azerty," not "0123456789," or not "abc123"), but try to combine lower- and uppercases with numbers and special characters (e.g., with a question mark or dashes). Alternatively, a combination of words or a sentence can be used.
- **Unique use**. Internet users should use a unique password per account and update it regularly, even if it will result in a long list of passwords. In order to remember all different passwords of all online accounts, a trusted password manager can be used (instead of saving them in a text file on your computer). Many online tools also allow their users to proactively add recovery options in case someone forgets his/her password.
- **Extra**. If possible, Internet users should use biometrics (e.g., a scan of their iris or fingerprint) or a multistep or multifactor authentication process to log in (e.g., with a unique code to be received on a cell phone, in addition to the password).
- **Privacy**. When using social media on someone else's computer, make sure to uncheck the "remember my password" function, and never let an account opened without the user's surveillance. Extra caution is needed when using public computers.

Strong and unique passwords are crucial in a social era where someone's digital life is an extension of his/her offline life. For instance, today, passwords are needed for all types of online activities, such as online banking or e-commerce, but also to get access to a computer, a cell phone, social media tools, or services in the cloud. The following videos are meant to make people aware that their entire life can be found online (i.e., by collecting information about a certain individual from different social media tools by means of social engineering) and that online information can be used against you:

- Example 1: amazing mind reader reveals his gift (http://www.youtube.com/watch?v=F7pYHN9iC9I)
- Example 2: how freaks can easily take over someone's life (http://www.youtube.com/watch?annotation_id=annotation_202513&feature=iv&src_vid=F7pYHN9iC9I&v=Rn4Rupla11M)

Consequently, it is highly important for Internet users to use social media and other online services in a privacy-friendly way. Social engineering also explains why Internet users should not use passwords that contain the name of their pet, child, or favorite movie, as those data might be easy to find on social media.

11.4 Takeaways

A final ethical note is dedicated to the reader in particular. As a social media user, each individual remains responsible for his/her social media behavior. Though, an organization can discipline its employees by means of a policy related to social media and IT in general. Nonetheless, proper use of social media and IT should be built on a relationship of mutual respect, trust, and loyalty.

Social media users have the right to get privacy and freedom of speech, albeit only to a certain extent. For instance, if information is really private, then you should not post it on social media and create digital evidence for it. Or as a matter of common sense, never insult others or never harm current and former employers. If necessary, the police will be able to track and trace online users, even if they have an anonymous account (e.g., based on the IP address of a computer, cookies in a browser, etc.). The latter is also true for online abuse outside a business context, such as cyberbullying among teenagers or pedophilia. The indirect or distant use of social media might give users a false sense of omnipotence.

Consequently, the message of this chapter is to act professionally and then a proper use of social media is likely to follow. Although an ethical behavior on social media contributes to online reputation management, the reader is encouraged to meet his/her online connections also in real life. As such, online and offline relationships can reinforce one another. In order to have more time for offline relationships and avoid a social media addiction, the reader might consider to check social media updates only at fixed moments in time (e.g., once in the morning, once at noon, and/or once in the evening).

11.5 Self-Test

- Can you explain the dangers related to social media use for organizations and employees?
- Do you know what a social media policy consists of?
- Can you recognize the difference between ethical and unethical use of social media in real-life situations?
  - Is it ethical for an organization to counter online criticism and defend its online reputation?
  - What if an employee has blogged about his colleagues without mentioning any names?

  - What would you do if your employer asks you to put information on the corporate website and on social media without referencing or acknowledging the original sources?
  - Can an employee present himself/herself as an official representative of or a spokesperson for an organization?
  - George worked for 5 years as the Chief Social Media Officer at organization XYZ, before becoming a freelance. He intends to write a personal blog post that contains copyrighted information belonging to his former employer, organization XYZ. What should George do to act ethically correct?
- Can you think of unethical actions that an organization should avoid when promoting products or services online?
- Do you know the importance of strong passwords for social media?
- Can you explain how password hijackers can profit from social engineering?

Bibliography

Association of Corporate Counsel. (2010). *The risks of social media usage in the workplace*. Retrieved July 28, 2014, from: http://www.lexology.com/library/detail.aspx?g=48457319-7f27-44a9-98bf-d0a93e1bbb36

Bélanger, F., & Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041.

Borremans, P. (2013). [Guest lecture of Philippe Borremans in the course Creating Value Using Social media at Ghent University, December 2013].

Boudreaux, C. (2014). *Social media policy database*. Retrieved July 28, 2014, from: http://socialmediagovernance.com/policies/

BullGuard. (2013). *What you need to know about passwords*. Retrieved June 15, 2013, from: http://blog.bullguard.com/2013/04/what-you-need-to-know-about-passwords.html

Burnett, M., & Kleiman, D. (2006). *Perfect passwords: Selection, protection, authentication*. Rockland: Syngress Publishing.

Carroll, E., & Romano, J. (2010). *Your digital afterlife: When Facebook™, Flickr and Twitter are your estate, what's your legacy?* Berkeley: Pfeiffer.

CNET. (2011). *How to set up Google's Inactive Account Manager*. Retrieved June 17, 2013, from: http://www.cnet.com/how-to/how-to-set-up-Googles-inactive-account-manager/

Flynn, N. (2012). *The social media handbook: Rules, policies, and best practices*. San Francisco: New Riders.

Forbes. (2012). *Should all social media managers be under 25?* Retrieved June 16, 2013, from: http://www.forbes.com/sites/kellyclay/2012/07/23/should-all-social-media-managers-be-under-25/

HR Examiner. (2013). *Social media's real legal issues*. Retrieved June 16, 2013, from: http://www.hrexaminer.com/social-medias-real-legal-issues/

Institute of Business Ethics. (2011). *The ethical challenges of social media*. Retrieved July 28, 2014, from: http://www.ibe.org.uk/userassets/briefings/ibe_briefing_22_the_ethical_challenges_of_social_media.pdf

Intel. (2013). *Are you hackable or uncrackable? Play our password game*. Retrieved June 15, 2013, from: https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html

Jain, T. K. (2013). *Ethics and social media*. Retrieved June 15, 2013, from: http://www.Slideshare.net/kmtj1979/ethics-and-social-media-18628942

Postman, J. (2009). *SocialCorp: Social media goes corporate*. Berkeley: New Riders.

Reynolds, G. W. (2010). *Ethics in information technology*. Boston: Course Technology, Cengage Learning.

Social Media Explorer. (2014). *Are you prepared for your digital afterlife?* Retrieved July 28, 2014, from: http://www.socialmediaexplorer.com/social-media-marketing/are-you-prepared-for-your-digital-afterlife/

SocialMedia.org (2010). *The SocialMedia.org disclosure toolkit*. Retrieved June 15, 2013, from: http://socialmedia.org/disclosure/

Stop Blocking! (2010). *B.L. Ochman offers five reasons for open access*. Retrieved July 29, 2014, from: http://www.stopblocking.org/?p=87

Terms of Service; Didn't Read. (2013). "*I have read and agree to the Terms" is the biggest lie on the web. We aim to fix that*. Retrieved June 18, 2014, from: http://tosdr.org/index.html#services

The Digital Beyond. (2010). *Your digital afterlife*. Retrieved June 15, 2013, from: http://www.youtube.com/watch?feature=player_embedded&v=0_xV9UfCLXA#t=70

Velasquez, M., Andre, C., Shanks, T. & Meyer, M. J. (2009). *A framework for thinking ethically*. Retrieved July 29, 2014, from: http://www.scu.edu/ethics/practicing/decision/framework.html

Vuze. (2013). *Six digital afterlife services to help you prepare for your death*. Retrieved July 28, 2014, from: http://blog.vuze.com/2013/12/13/6-digital-afterlife-services-help-prepare-death/

Wikipedia. (2014). *Copyright*. Retrieved July 28, 2014, from: http://en.wikipedia.org/wiki/Copyright

Word of Mouth Marketing Association. (2014). *WOMMA ethics committee white paper*. Retrieved July 28, 2014, from: http://www.womma.org/ethics